UDC 004.42
IRSTI 81.93.29

METHOD OF CONSTRUCTING MODELS OF INFORMATION ATTACKS

Barakova A.Sh., Ussatova O.A.

Institute of Information and Computational Technologies, Almaty, Kazakhstan,
Al-Farabi Kazakh National University, Almaty, Kazakhstan
balia_79@mail.ru
uoa_olga@mail.ru
ORCID ID: https://orcid.org/0000-0002-5276-6118
ORCID ID: https://orcid.org/0000-0002-0904-745X

Abstract. The existing approaches to the construction of formal models of information attacks are considered and analyzed. The basic requirements for information attack models are formulated. A method is proposed for constructing models of information attacks based on control E-network transitions and multi-agent management, taking into account the formulated requirements. The considered approaches to modeling allow describing the process of an information attack with varying degrees of detail. The models use different mathematical bases, but most of them are based on finite automata and represent the attack as a sequence of automaton states. None of the models makes it possible to take into account the vulnerability activated by such a complex, the method of its implementation and possible consequences. The models allow us to more accurately determine the effectiveness of existing and developed means of protection against simulated information attacks.

Keywords: attack, modeling, information attack model, managing E-network, agent, multi-agent management.

Introduction

Currently, one of the most relevant areas of scientific research in the field of information security is the development of methods and tools for detecting attacks and protecting against attacks on computer systems and networks. In the process of such development, it is necessary to constantly conduct research, including preliminary study and detailed study of possible options for implementing information attacks. As a rule, these works are carried out using models that allow reproducing the necessary properties and characteristics information attack, as well as to assess the level of its danger to the computer system (CS). The models allow us to more accurately determine the effectiveness of existing

The currently created models of information attacks can be classified according to the following basic criteria [1]:

– the possibility of expanding the model (models with a fixed number of parameters and their values, extensible models with the possibility of adding new parameters and their values);

– the possibility of taking into account the sequence of actions performed in an information attack in the model;

– the level of detail of the model (models of low, medium and high level of detail). and developed means of protection against simulated information attacks.

A formalized information attack model based on attack trees developed by B. Schneier has become widespread [2]. Attack trees are conceptual diagrams that describe threats to the system and possible

attacks aimed at their implementation. The underlying construction here is a hierarchical tree G =(L,E), where

{ }i L = l is the set of tree vertices,

{ }s E = e ,

2 E ⊂ L – the set of tree arcs
Each vertex of the tree G is associated with a certain action of the violator, while the root of the tree denotes the ultimate goal of an information attack, the implementation of which can cause significant damage to A C. Thus, it is possible to make up a set of possible paths on the graph G { }i Gp = gp , where each path i gp is a sequence of arcs) (, , ..., 1 2 n e e e of the form ei = (. li,lj), li,l j ∈ L In this case , the final vertex of the arc i l is simultaneously the initial vertex of the arc l_{i+1} .

The leaves of the tree G can act as the initial vertex of the path, and the root of the tree can act as the final vertex. The Schneier attack tree model has several important advantages and disadvantages

Advantages	**Disadvantages**
– the model can be used to describe attacks on any informationor physical systems; – due to the presence of numerical values at the vertices and edges, the model provides an opportunity to introduce estimates of each step according to certain criteria, for example, by execution time, number of operations, estimated cost, etc. The sequence of steps can be evaluated based on the criteria of each step; – the expansion of the attack model is carried out by adding new elements to the sets of vertices and arcs of trees describing the attack; – it is possible to simulate complex information attacks involving several implementation options.	This model has a number of disadvantages, which should include: – a tree is used as a fundamental structure for modeling an attack, which imposes some restrictions on the structure of the graphical representation of the model. The presence of cycles also creates certain difficulties when working with this model; – the attack model does not include the parameters of the AU environment, under which the implementation of the simulated attack is possible; – there are no tools in the model that provide dynamic modeling.

In [3], a formal method of attack modeling is proposed, which is an extension and refinement of the model based on the attack tree. Two attributes are introduced: the lifetime (reflects the time dependencies between the stages of the attack) and the degree of confidence (characterizes the probability of reaching the target of the attack with the achieved sub-targets). However, this model has the same disadvantages as those based on the attack tree. The attack graph model [4] is also based on an extension of the attack tree model. Attack graphs are a specialized tool for describing an attack. Graph nodes do not represent conceptual actions, but network nodes, program processes, configuration files, code sections, etc. The model is widely used because it is based on a simple and well–researched mathematical base - finite automata, itself is quite simple and obvious. Transitions between nodes are carried out on based on deterministic rules, the current value of some system parameters, variables, etc. may be taken into account. Existing graph models are wellsuited for describing the sequence of actions of an attacker and are often used to assess the complexity of an information system security breach, rather than formodeling and investigating attacks. The disadvantages of these models can also be attributed to the fact that they do not contain

mechanisms for organizing controlled branching and modeling the dynamic component of the attack.

Information attack models are also built on the basis of formal languages and ontologies [5]. Formally, the ontology is a tree, and the threat is represented by a sequence of symbols. Sequences are considered as words of a formal language specified by means of some formal grammar. The description of the generalized attack scenario by means of stochastic grammar has the following form

$$GA = (V_N, V_T, S, P) \quad (1)$$

where VN is a set of non–terminal symbols that denote micro–level attack steps, VT is a set of terminal symbols that correspond to the upper and intermediate levels of representation of the attack scenario steps, S is the initial symbol of the attack scenario, P is a set of output rules describing the operations of detailing the attack scenario by replacing characters. Each replacement is carried out with a given probability:

$$\alpha_i \rightarrow \beta_{ij}\ ,\ = 1,...,\ ,\ = 1,...,\ , \quad (2)$$

where a_i is a nonterminal character, β_{ij} is a string of terminal and nonterminal characters

It is characteristic that the conceptual model of information attack based on formal languages and ontologies is in many ways similar to the model discussed above, developed by B. Schneier. The model is also represented as a graph structure and can be expanded by adding new elements to the sets of terminal and non-terminal symbols, as well as by expanding the output rules. The model can be presented both in text and graphical form. The main disadvantage of such an information attack model is the absence of a parameter that characterizes the vulnerability of the CS, on the basis of which the violator's action is performed.

Requirements for information attack models

For effective use in order to study the likely actions of the violator in relation to the CS, the information attack model being developed must meet the following minimum set of requirements:

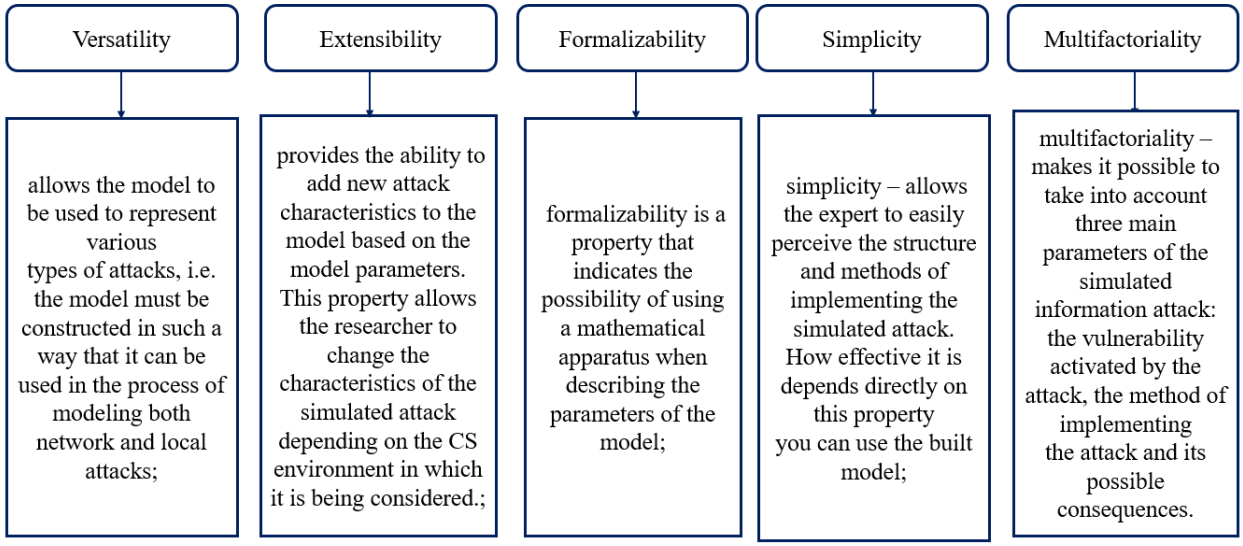


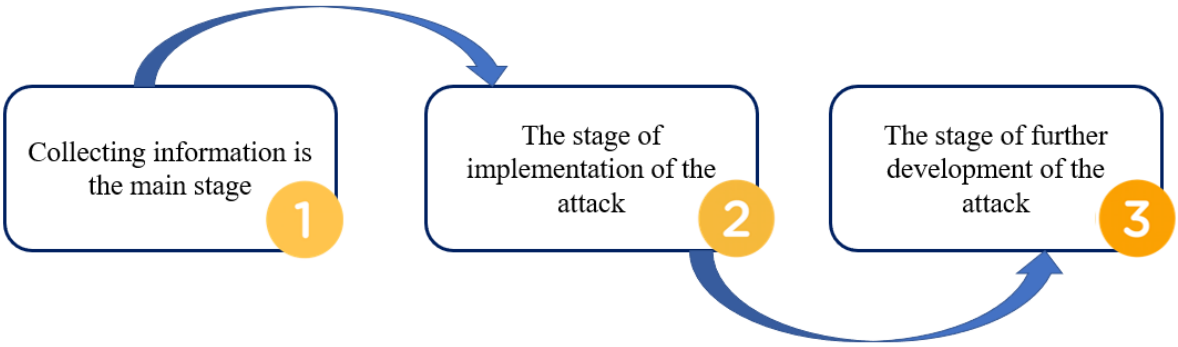
Figure 1 - Requirements for information attack models

Information attack as a modeling object

An attack on an information system is an action or sequence of related actions of an intruder that lead to the realization of a threat by exploiting system vulnerabilities. Vulnerability is

commonly understood as the weak point of the CS, on the basis of which the successful implementation of the threat is possible. In turn, a threat is a potentially possible event, action, phenomenon or process that can cause
damage to the system resource [6]. Thus, in order to implement the attack, the attacker simulates some action that leads to the desired result with the help of some means that exploits the vulnerabilities of the system.

In general, an information attack can consist of three stages:



1. Collecting information is the main stage. At this stage, the target of the attack is selected, information about it is collected (OS, configuration, services), the mostvulnerable places of the attacked system are identified, the impact on which leads to the desired result, the type of attack being implemented is selected.

2. The stage of implementation of the attack. At this stage, the violator gets unauthorized access (ND) to the resources of those CS nodes in relation to which the attack is carried out. If, by the nature of the impact, the attack is active [7], then this stage is also accompanied by the realization of the goals for which the attack was undertaken. The resultof such actions may be a violation of confidentiality, integrity and availability of information. In addition, at this stage, the source andthe fact of the attack may be hidden, the so-called "covering up traces".

3. The stage of further development of the attack – actions are performed that are aimedat continuing the attack on the resources of other CS nodes. In the case of passive attacks [7], this stage is the stage of completing the attack.

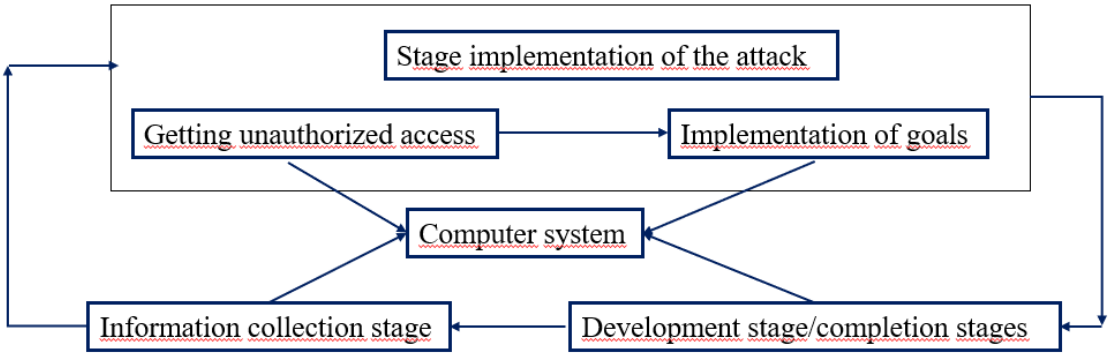


Figure 2 - schematically shows the stages of the life cycle of a typical information attack.

When modeling an information attack, it is necessary to determine its parameters and characteristics. The main parameters of the attack are:
– duration of action;
– multiplicity;
– a list of vulnerabilities used by the attack.
Note that modeling some types of attacks, for example, "distributed denial of service" – DDoS requires

the definition of additional attack parameters, such as [8]:
– type of attack (semantic attack (TCP SYN, Incorrect packets, Hard request, etc.)
or "brute force" type attack – such as UDP/ICMP flood, smurf/fraggle, etc.);
– rate of attack (can be constant or variable. In the latter case, the intensity of the attack varies over time. The change in tempo can be increasing or fluctuating);
– influence on the target of the attack (you can choose a "disruptive" attack, when a distributed attack will be carried out from all attacking nodes at once, or a worsening one – the number of attacking nodes is included in the attack gradually. The first attack option is easier to detect);
– the constancy of the set of attacking nodes (the set can be constant (the same nodes attack) or variable);
– the degree of automation (automatic or automated).

The proposed method of modeling attacks

Taking into account the disadvantages of existing analogues, we will use Control E-Nets (Control E-Nets – CEN) as an information attack model [9, 10], which are a modification of E-networks and meet all the requirements for the attack models described above. Issues of the complexity of the attack model (taking into account the vulnerability search stage in attack models, methods of implementation and development of the attack) will be solved using a multi-agent control system, the modules of which work on the principles of intelligent agents. We will describe each agent using the implementation model presented in viRis. 1. The life cycle of a typical information attack on CS resources de managing E-network. We will simulate attacks in a specially designed environment, which is based on the principles of invariance to the subject area, the level of modeling, the experiment being conducted and the level of user readiness. Let's consider in more detail the mechanisms of operation of the control E-networks, systems multi-agent management and information attack simulation environment.

Conclusions

A method of constructing information attacks based on control E-networks and multi-agent management is proposed. Using this method allows you to create models based on simple, easily perceived constructions to represent various types of attacks. Thanks to the use of the mechanism of control E-networks, the method allows you to take into account the current state of the CS and the object of attack during modeling – dynamic modeling is provided.

In addition, the control E-networks allow the use of mathematical apparatus when describing the parameters of the model – the property is provided formalizability of the model. The use of a multi-agent approach makes it possible to solve the problem of multifactorial (complexity) attacks, highlighting the stage of finding vulnerabilities of attack objects (planning level), the stages of implementing the attack and determining its possible consequences (reactive level); there is a cooperative level for the exchange of information between agents of different levels. The obtained simulation models of information attacks can be used to build a synthetic environment of information security systems in order to clarify their features and characteristics using the method of semi-natural modeling.

References

[1] Serdyuk V. A. Analysis of modern trends in building models of information attacks. Information technology. 2004. 5. 94-101.

[2] Schneier B. Attack Trees [Electronic resource] Availability mode:
http://www.schneier.com/paper-attacktrees-ddj-ft.html.

[3] Campete S. A formal Method for Attack Modeling and Detection: Availability mode: http://citeseer.ist.psu.edu/751069.html [Electronic resource]

[4] Shener O. Automated Generation and Analysis of Attack Graphs. USA, 2002. 273 – 284.
[5] Gorodetski V. Attacks against Computer Network: Formal Grammer-based Framework and SimulationTool. Proceedings of the international RAID conference. St. Petersburg, 2002. 219-238.
[6] Lukatsky A.V. Detection of attacks. St. Petersburg: VVH-Petersburg, 2001. 624.
[7] Natrov V. V. Classification of network attacks. Information technologies in Management and modeling: SAT. Dokl. Belgorod, 2005. 128-132.
[8] Kotenko I. V. Modeling the resistance of software agents on the Internet: a general approach, modeling environment and experiments. Information protection. INSIDE. 2006. 5. 2-10.
[9] Kazimir V. V. modeling of synthetic environment for reactive systems. Mathematical modeling. 2003. 2 (10). 24-32.
[10] Kazimir V. V. Model-oriented management of intellectual production systems: Dissertation of the Doctor of Technical Sciences: 05.13.06. 2006. 301.

АҚПАРАТТЫҚ ШАБУЫЛ МОДЕЛЬДЕРІН ҚҰРУ ӘДІСІ

Баракова А. Ш., Усатова О. А.

Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан,
Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
balia_79@mail.ru
uoa_olga@mail.ru
ORCID ID: https://orcid.org/0000-0002-5276-6118
ORCID ID: https://orcid.org/0000-0002-0904-745X

Аңдатпа. Ақпараттық шабуылдардың формальды модельдерін құрудың қолданыстағы тәсілдері қарастырылып, талданды. Ақпараттық шабуыл модельдеріне қойылатын негізгі талаптар тұжырымдалған. Электрондық желінің бақылау ауысуларына және тұжырымдалған талаптарды ескере отырып, мультиагентті басқаруға негізделген ақпараттық шабуыл модельдерін құру әдісі ұсынылды. Қарастырылған модельдеу тәсілдері ақпараттық шабуыл процесін әртүрлі дәрежеде егжей-тегжейлі сипаттауға мүмкіндік береді. Модельдер әртүрлі математикалық негіздерді қолданады, бірақ олардың көпшілігі ақырғы машиналарға негізделген және шабуылды А ретінде ұсынадыавтомат күйлерінің реттілігі. Модельдердің ешқайсысы мұндай кешен арқылы іске асырылатын осалдықты, оны жүзеге асыру тәсілін және ықтимал салдарын ескеруге мүмкіндік бермейді. Модельдер қолданыстағы тиімділікті дәлірек анықтауға мүмкіндік береді және имитациялық ақпараттық шабуылдардан қорғау құралдары

Кілттік сөздер: шабуыл, модельдеу, ақпараттық шабуыл моделі, электрондық желіні басқару, агент, мультиагентті басқару.

СПОСОБ ПОСТРОЕНИЯ МОДЕЛЕЙ ИНФОРМАЦИОННЫХ АТАК

Баракова А.Ш., Усатова О.А.

Институт информационных и вычислительных технологий, Алматы, Казахстан,
Казахский Национальный университет имени Аль-Фараби, Алматы, Казахстан
balia_79@mail.ru
uoa_olga@mail.ru
ORCID ID: https://orcid.org/0000-0002-5276-6118
ORCID ID: https://orcid.org/0000-0002-0904-745X

Аннотация. Рассмотрены и проанализированы существующие подходы к построению формальных моделей информационных атак. Сформулированы основные требования к моделям информационных атак. Предложен метод построения моделей информационных атак, основанный на контрольных переходах электронной сети и мультиагентном управлении, с учетом сформулированных требований. Рассмотренные подходы к моделированию позволяют описать

процесс информационной атаки с разной степенью детализации. Модели используют различные математические основы, но большинство из них основаны на конечных автоматах и представляют атаку как последовательность состояний автомата. Ни одна из моделей не позволяет учесть уязвимость, активируемую таким комплексом, способ ее реализации и возможные последствия. Модели позволяют нам более точно определять эффективность существующих и разрабатываемых средств защиты от имитируемых информационных атак.

Ключевые слова: атака, моделирование, модель информационной атаки, управляющая электронная сеть,агент, мультиагентное управление.

Сведения об авторах:

Англ: Olga Aleksandrovna Ussatova, PhD, Institute of Information and Computational Technologies, Almaty, Kazakhstan

Каз: Усатова Ольга Александрқызы,философия докторы,Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан

Рус: Усатова Ольга Александровна,доктор философии, Институт информационных и вычислительных технологий, Алматы, Казахстан

Англ:Aliya Sharizatovna Barakova, doctoral student, Al-Farabi Kazakh National University, Almaty, Kazakhstan

Каз: Баракова Алия Шаризатқызы, докторант, әл-Фараби атындағы ҚазҰУ, Алматы, Қазақстан

Рус: Баракова Алия Шаризатовна, докторант, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан.