http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

D2-02_09

Construction of Next-generation Security Infrastructure to Cope with New Types of Cyber Attacks

Takehiro Sueta*
Kyushu Electric Power Co., Inc.

Haruki Terakura
NEC Corporation

(JP)

SUMMARY

Electric power companies hold confidential information including customer and nuclear generation facility-related information and, therefore, implement security measures to prevent damage such as information breaches in the event of a cyber attack.

Cyber attacks have recently transformed from general, non-specific target types to target-specific types that aim to exploit specific information, rendering it difficult to prevent damage by using conventional security measures. To cope with this situation, security measures need to be reinforced to prevent damage in the event of cyber attacks.

This paper organizes and provides knowledge about next-generation security measures introduced by Kyushu Electric Power Company (KEPCO) to prevent leakage of confidential information with the focus on the content of communications transmitted by PCs infected with malware to external servers.

KEYWORDS

Virus Definition File, Pattern Matching, Targeted Attack, Targeted E-mail Attack, Vulnerability, Zero-day Attack, Next-generation Security Infrastructure, Outbound Content Security, Bot

* 1-82, Watanabe-dori 2-Chome, Chuo-ku, Fukuoka, 810-8720 Japan.
Fax: + 81-92- 761-7749 e-mail: Takehiro_Sueta@kyuden.co.jp

1. Background and Purpose

Electric power companies hold confidential information including customer and nuclear generation facility-related information. To prevent damage such as the exploitation of such information due to cyber attacks that infect in-house servers and PCs with malware, the main approach is to implement security measures by applying pattern matching based on comparison with Virus definition files. This approach blocks illegal communication at the point of connection between an external network (Internet) and the in-house OA network to prevent incursion of malware into the company.

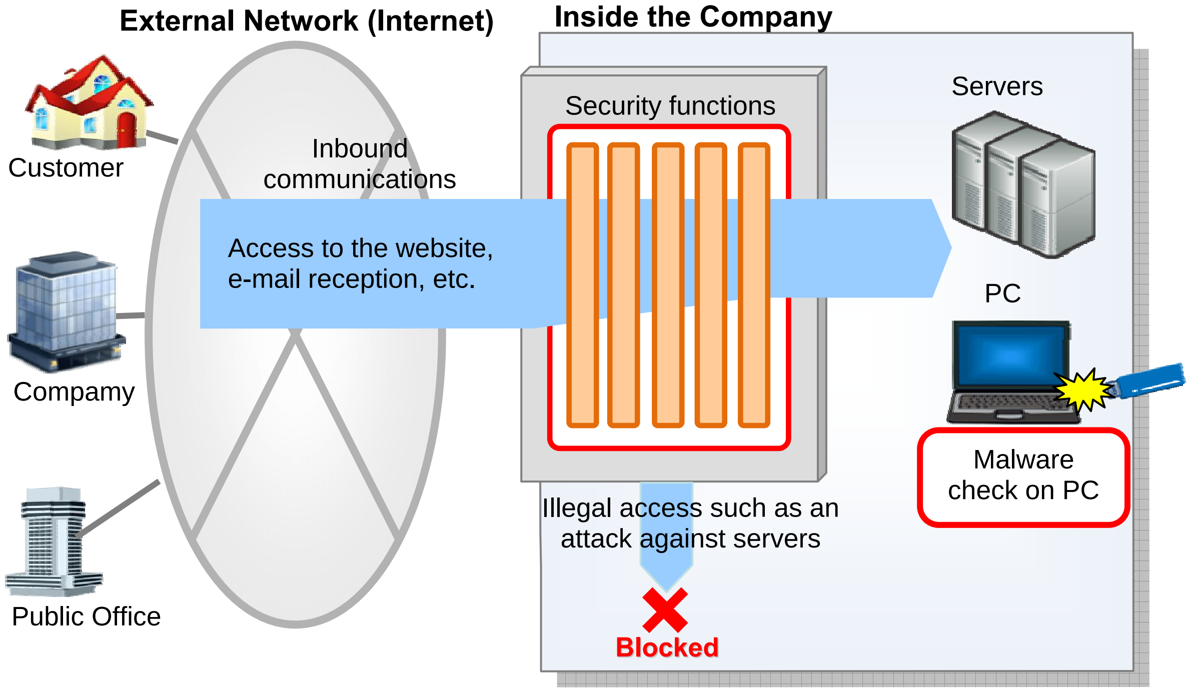


Fig. 1 Overview of Existing Security Measures

Although KEPCO has also implemented pattern matching-based security measures, this approach presents the problem of unknown malware not identified in virus definition files being allowed to penetrate the company.

Cyber attacks have recently transformed from general, non-specific target types to target specific types that aim to exploit specific information, rendering it difficult to prevent damage by using conventional pattern matching-based security measures alone.

To cope with this situation, KEPCO has reinforced its security measures to prevent confidential information security breaches even in the event of infection by malware undetectable by pattern matching-based security measures.

2. Overview of Security Measures and Current Issues in Japan

Unlike general, non-specific target attacks, targeted attacks are aimed at specific organizations or groups and this means that the method of attack is specially designed to penetrate the target entity. For this reason, since the aims of attackers are changing and attack methods are becoming more sophisticated, it is difficult to prevent damage from such attacks by using security measures (e.g. firewalls and anti-virus software) that have been the norm to date premised on general, non-specific target attacks.

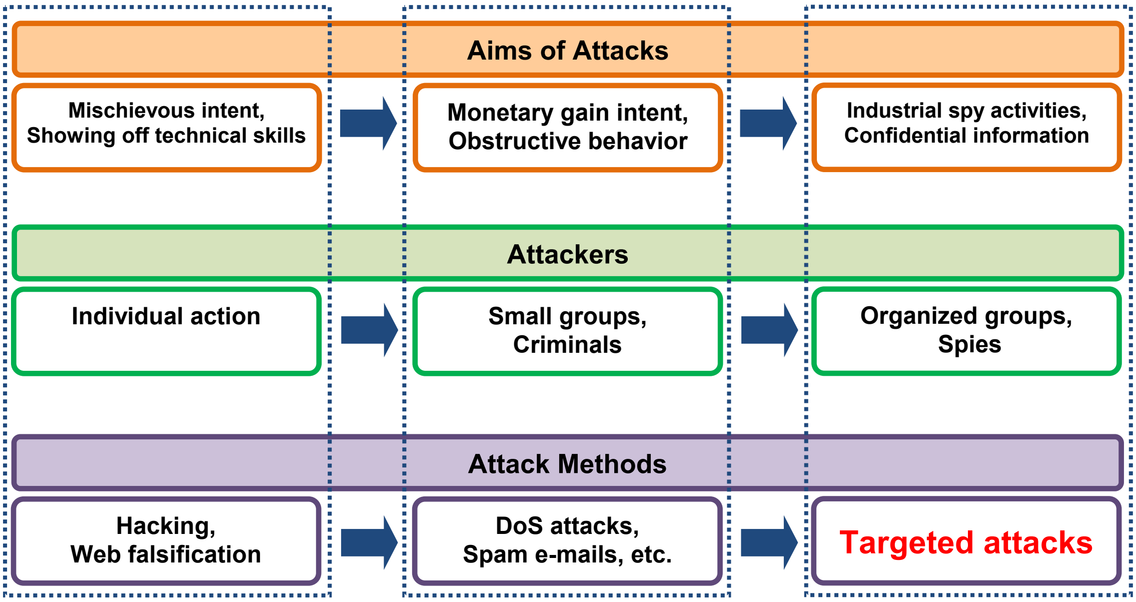

Aims of Attacks
Mischievous intent, Showing off technical skills
Monetary gain intent, Obstructive behavior
Industrial spy activities, Confidential information
Attackers
Individual action
Small groups, Criminals
Organized groups, Spies
Attack Methods
Hacking, Web falsification
DoS attacks, Spam e-mails, etc.
Targeted attacks

Fig. 2 Changes of Cyber Attacks

In concrete terms, targeted attack techniques are cleverly designed to trick users by combining multiple techniques such as “targeted e-mail attacks” that initiate malware infection when attached files or URLs are clicked and “zero-day attacks” that take advantage of unfixed vulnerabilities and are capable of efficient and long-term span execution.

Generally, targeted attacks employ the following techniques:

0. Preparation

   Collection of information on the target (and its surroundings) and the environment used for the attack

1. Misrepresentation (Targeted e-mail attacks, address misrepresentation, PC hijacking)

   In the guise of a friend of the target or an authoritative organization, the attacker accesses the target by e-mail.

2. Opening file attachments

Opening of a file attachment by the target (Malware is concealed in the file attachment.)

3. Information communication, operation, data exploitation and concealment
   A foundation for the attack is built using a back door to exploit the target information, and all traces of the attack deleted using the acquired administrator privileges. (Log falsification)

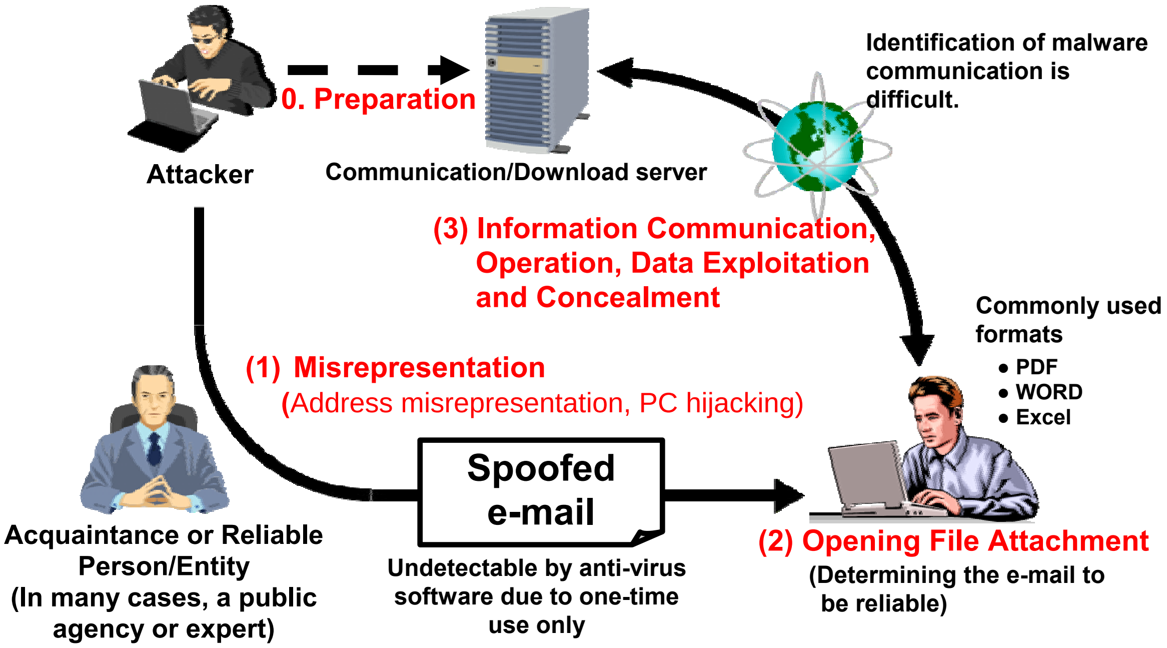

Identification of malware communication is difficult.
0. Preparation
Attacker
Communication/Download server
(3) Information Communication, Operation, Data Exploitation and Concealment
Commonly used formats
● PDF
● WORD
● Excel
(1) Misrepresentation
(Address misrepresentation, PC hijacking)
Spoofed e-mail
Acquaintance or Reliable Person/Entity
(In many cases, a public agency or expert)
Undetectable by anti-virus software due to one-time use only
(2) Opening File Attachment
(Determining the e-mail to be reliable)

Fig. 3 Common Method of Targeted Attacks

Further reinforcement of existing security measures, for example, by strengthening operational administrative measures (improved information literacy of employees and establishment of information sharing/security systems) and technical measures (timely updates of anti-virus software definition files and prompt application of programs to correct problems with operating systems/applications) enables enhancement of the security level of the organization concerned. However, total prevention of damage caused by malware infections is almost impossible. For this reason, to minimize damage caused by increasingly sophisticated cyber attacks, construction of the next-generation security infrastructure is required for each company.

3. Construction of Next-generation Security Infrastructure

As described in the previous section, foolproof prevention of malware infections is difficult, even with reinforced security measures. In the future, not only countermeasures to prevent malware from penetrating the company, but also mechanisms to detect malware infection of in-house servers and PCs will need to be put in place and implemented. To meet these needs, KEPCO has introduced an outbound content security system that can detect malware infections with the focus on the content of communications transmitted by malware-infected PCs to external servers and details of the system are presented below.

3.1. Overview of Outbound Content Security System Functions

The outbound content security system detects the activities of a PC infected with malware (bot) that acts on the commands received from the external command-issuing server by constantly monitoring and analyzing communication packets at the point of connection between an external network (Internet) and the in-house OA network.

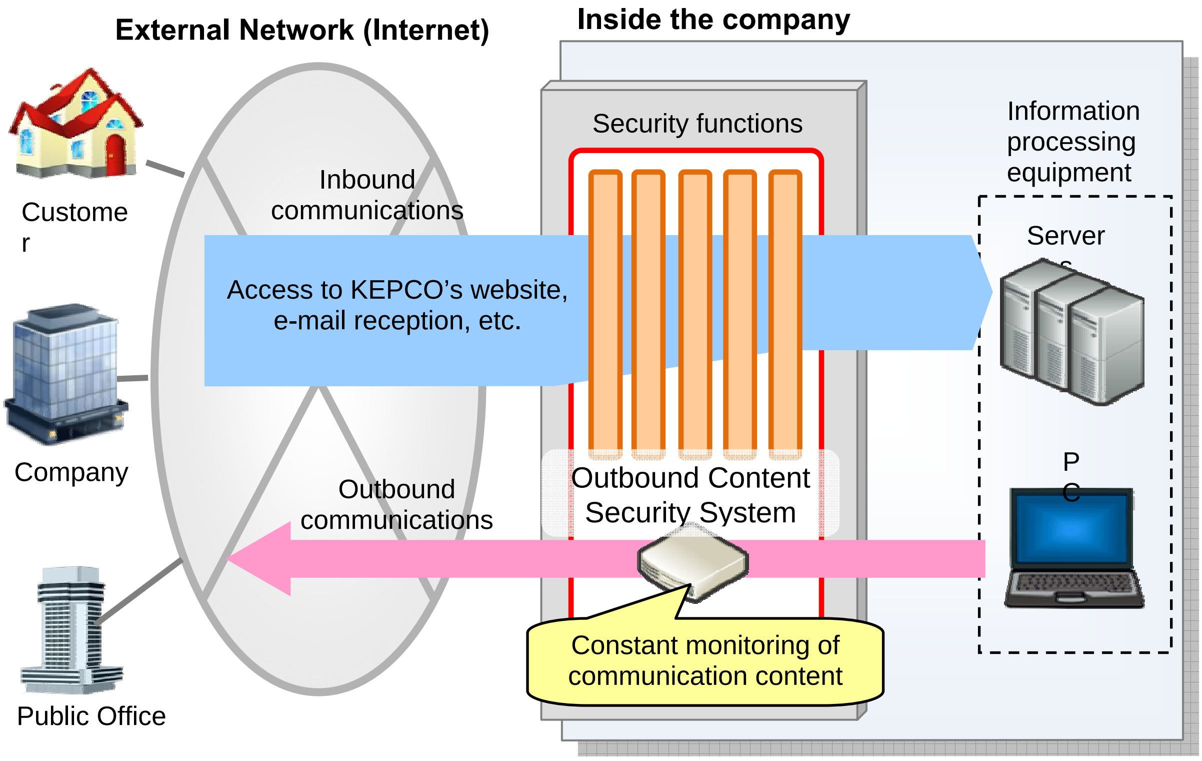


Fig. 4 Overview of Security Measures after Introduction of Outbound Content Security System

The main items of communication content detected by the outbound content security system are listed below.

- Communication implemented by a bot-infected PC to connect to an external command-issuing server (comparison with IP addresses in the database)
- Communication patterns implemented by a bot-infected PC such as keep-alive transmissions (comparison of communication pattern information in the database with communication packets)
- IP address scanning behavior for the purpose of examining the internal network

A bot-infected PC will firstly investigate details such as types of devices existing in the network, the configuration of device connections and available communication paths. Based on this information, the attacker then locates points that are vulnerable to attacks and estimates the location of attack-targets such as AD servers that manage account information and file servers containing internal information. Since this process will invariably trigger communication with the command-issuing server, this can be used to identify and investigate the corresponding terminal at the point at which communication was first detected, thereby preventing breaches of confidential information.

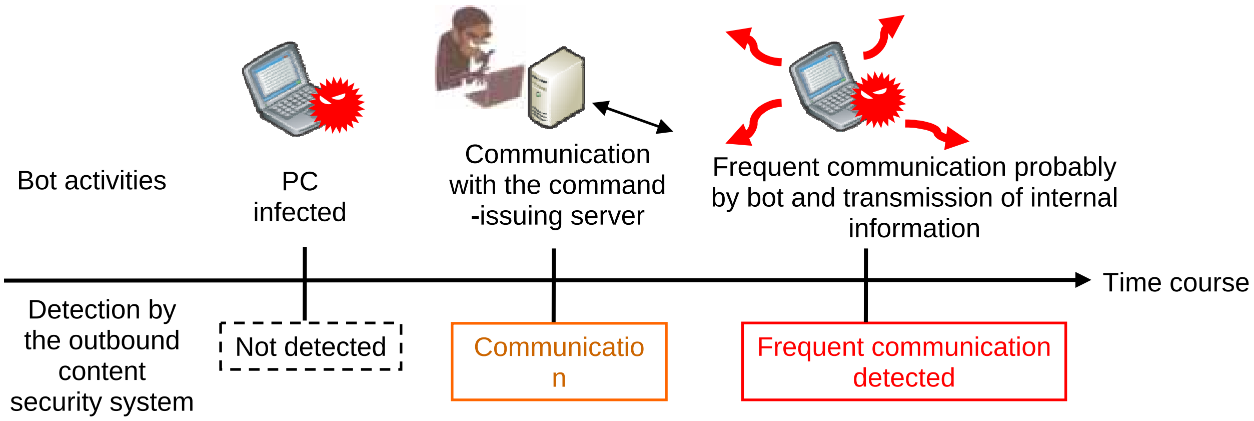
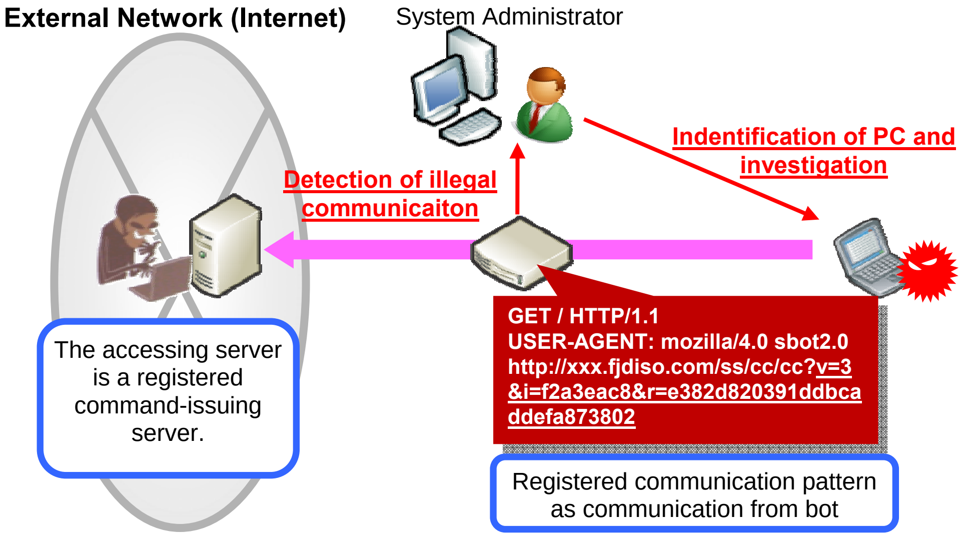

Bot activities
PC infected
Communication with the command -issuing server
Frequent communication probably by bot and transmission of internal information
Time course
Detection by the outbound content security system
Not detected
Communicatio n
Frequent communication detected

Fig. 5 Bot Activities and Detection by the Outbound Content Security System

3.2. Operational Status and Evaluation at KEPCO

3.2.1. Operating Method

KEPCO launched operation of the outbound content security system in August 2012. Notification of details of any illegal communication detected by the system is sent to the system administrator.


External Network (Internet)
System Administrator
Indentification of PC and investigation
Detection of illegal communicaiton
The accessing server is a registered command-issuing server.
Registered communication pattern as communication from bot

```
GET / HTTP/1.1
USER-AGENT: mozilla/4.0 sbot2.0
http://xxx.fjdiso.com/ss/cc/cc?v=3
&i=f2a3eac8&r=e382d820391ddbca
ddefa873802
```

Fig. 6 Outbound Content Security System Operating Method

Detected illegal communications are classified into several types based on bot activity events as shown in the table below. In addition, the outbound content security system performs correlation analysis of the detected activity event and, in the event that there is a possibility of bot infection, puts the corresponding PC into “Possible bot infection” or “Active bot” status on the system.

Type of Illegal Communication		Details of Detection by Outbound Content Security System
Bot activity events	Communication with command-issuing server	Detection of communication transmitted to the IP address of bot’s command-issuing server
	Communication by bot	Detection of bot communication patterns such as keep-alive transmissions
	Malware download	Detection of communication to download malware from a malware-containing site
	IP address scanning	Detection of large volumes of communications transmitted to a wide range of IP addresses using a specific protocol within a fixed period of time
	Spam e-mail transmission	Detection of transmission of large volumes of SMTP communications
Bot status	Possible bot infection	Detection of bot activities and determination of possibility of bot infection
	Active bot	Frequent detection of bot activities and determination of active bot

Risk levels are defined as “low,” “medium” and “high” according to the types of illegal communications. The PC concerned is checked and the malware eliminated immediately in the event of “high” risks and within the following business day in the event that the risk is “medium” or “low.

3.2.2. Operational Status and Evaluation

So far, a number of incidents such as communication with command-issuing servers and communication for downloading of new malware from malware-containing sites have been detected, and investigation of the PCs concerned has resulted in determination of malware infection and subsequent elimination of the malware.

To facilitate penetration, the first invading malware is made small and, in many cases, is provided with a limited number of functions. Malware that has been eliminated as a result of detection of communication in the course of operation of the system at KEPCO also has functions that allow the malware to download other malware to enable remote control of infected PCs by the attacker, for example, and it is probable that the malware will be provided with other such functions required for the attack in the future.

In this way, the introduction of the outbound content security system has made it possible to quickly discover malware-infected PCs from the content of communications, even in cases where the malware is unknown and cannot be detected by the application of pattern matching, so that attacks can be nipped in the bud at the initial stage.

4. Summary and Future Issues

4.1. Summary

Up to the present, in cases of infection of in-house servers or PCs by unknown malware that is not identified by virus definition files, detection of infections has been impossible unless infected servers or PCs behave in an unusual manner. As a result, companies have been faced with the risk of exploitation of confidential information by attackers before they even realize that they have been targeted by cyber attacks.

The introduction of the outbound content security system described in this paper enables the detection of malware infections of in-house servers or PCs from the content of communications even if the malware concerned is unknown and not identified by virus definition files. As a result, it is now possible to discover the fact of malware infection at an early stage and prevent breaches of confidential information. Moreover, we believe that this system is also beneficial because of the fact that no detection of suspicious communications indicates the absence of malware infections and this, therefore, means that there has been no breach of confidential information.

4.2. Future Issues and Outlook

The outbound content security system has been designed based on the concept of detecting all possible malware infections and this presents the problem that, in some cases, the system overreacts to and detects even normal communications as communications carried out by malware. So far, there have been a number of cases in which, although communication with a command-issuing server has been detected, investigation of the PC concerned has revealed no malware infection, and that the destination of communications was a harmless site. Performing investigations of such incorrect detections caused by overreaction of the system has increased the system operation workload.

To address this problem, it was decided that, rather immediately investigating a PC on which a “low” level activity event has been detected, the PC concerned should be observed over a period of time. Even if the PC is infected with a bot, since its activities are still in the early stages, we believe that breaches of confidential information can be prevented by observing the PC over time and carrying out an investigation in the event of detection of subsequent continued activity events. In the future, we will continue to analyze the results of detection and decide on optimum detection criteria to reduce incorrect detections caused by overreaction of the system, taking into consideration the risk of breaches of confidential information and the system operation workload.