# Интегральные оценки защищенности информационно-телекоммуникационных систем

## Integral assessment of security of information and telecommunication systems

**Ключевые слова:** информационный ресурс – information resource; телекоммуникационная система – telecommunication system; оценка защищенности – protection assessment.

Статья посвящена проблеме защиты информационных ресурсов и процессов. Рассматриваются интегральные оценки защищенности информационно-телекоммуникационных систем.

This article deals with the problems of protection of information resources and processes. It includes a review of integral assessments of information and telecommunication systems security.

**СУХАНОВ / SUHANOV A.**
**Андрей Вячеславович**
(avsuhanov@eureca.ru)
доктор технических наук, профессор
Санкт-Петербургского национального
исследовательского
университета информационных технологий,
механики и оптики,
Санкт-Петербург

При создании информационно-телекоммуникационных систем (далее – ИТКС) естественным образом возникает проблема защиты информационных ресурсов и процессов. Не защитив ИТКС, мы сразу же становимся объектом атак различного рода хакеров, конкурентов и просто любителей навредить. При защите любой ИТКС необходимо ответить на три вопроса:

- **Что защищать?** Это значит, что для того, чтобы приступить к защите своей сети, нужно определить ее состав и сложность, а также важность информации, в ней циркулирующей.
- **От чего защищать?** Необходима оценка глобального и локального поля действующих угроз безопасности информации.
- **Как защищать?** Необходимо определить средства защиты, которые будут использованы при защите сети, необходимые и достаточные для отражения действующего множества угроз.

Для ответа на эти вопросы необходимо проведение детальных трудоемких исследований, которые позволят получить ориентировочную оценку интегрального уровня защищенности реального объекта. В таблице 1 приведены результаты оценок объемов циркулирующей и обрабатываемой информации на объектах информатизации. Таблица градуирует сложность объектов защиты в зависимости от оценки объема информации в ИТКС при различных уровнях сложности ее самой.

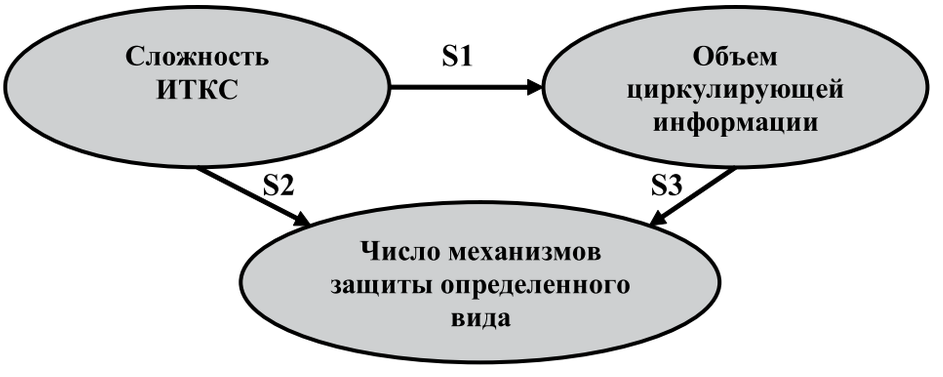
Очевидно, что если для самого низкого уровня требуются механизмы защиты (далее – МЗ) одного вида, то более высокому уровню требуются МЗ, используемые предыдущим уровнем, плюс дополнительные МЗ, обеспечивающие следующий уровень защищенности. Таким образом, возникает связь между сложностью системы, объемом циркулирующей в ней информации и числом МЗ определенного вида, показанная на рисунке.

Информационные ресурсы, присутствующие в ИТКС, различны. Это и документы, и графические файлы, и приложения, и программное обеспечение. Причем каждый уровень программного обеспечения включает свои МЗ. Следовательно, при росте сложности ИТКС растет номенклатура различных уровней программного обеспечения, каждое из которого использует свои виды МЗ. Таким образом, рост сложности ИТКС влечет за собой рост числа МЗ различных видов не только за счет увеличения структуры ИТКС, но и за счет увеличения видов программного обеспечения различного уровня, используемого в ИТКС.

Конечная цель анализа многофакторного пространства угроз, МЗ и сложности объекта защиты – получение интегральной сравнительной

Таблица 1

| Сложность ИТКС | Объем циркулирующей информации, Мбайт |
|---|---|
| Хост | $10^4$ |
| ЛВС | $10^7$ |
| КВС | $10^{10}$ |
| ГВС | $10^{20}$ |




Связь сложности ИТКС, объема циркулирующей в ней информации с числом МЗ определенного вида, используемых в ИТКС:
S1 – зависимость объема циркулирующей в ИТКС информации от сложности ИТКС;
S2 – зависимость числа МЗ определенного вида от сложности ИТКС;
S3 – зависимость числа МЗ от объема циркулирующей в ИТКС информации

оценки защищенности объекта. Способов получения такой интегральной оценки в виде единственного числа достаточно много. Приведем один из них, использованный на ряде объектов информатизации для получения объективной оценки уровня защищенности ИТКС при проведении аттестационных испытаний объектов информатизации [1].

В таблице 2 приведены параметры и их веса, использованные при анализе и оценке уровня защищенности (рейтинга защищенности) ИТКС. Для расчета интегрального сравнительного рейтинга использовались обозначения (табл. 3) и соотношение, приведенное ниже.

Таблица 2

| Показатели сложности ИТКС | | | Показатели сложности МЗ | | |
|---|---|---|---|---|---|
| **Метрики ИТКС** | | **Рейтинг** | **Метрики МЗ** | | **Рейтинг** |
| **1. Число компонентов** | | | **1. Сертифицированные МЗ** | | |
| 1.1. Цифровые АТС | 1 | 100 | 1.1. АС | 0 | 0 |
| | 5 | 500 | | До 5 | 7 |
| | 10 и более | 1000 | | Более 5 | 15 |
| 1.2. Серверные группы | 1 | 100 | 1.2. СВТ | 0 | 0 |
| | 5 | 500 | | До 5 | 7 |
| | 10 и более | 1000 | | Более 5 | 15 |
| 1.3. АРМ | До 100 | 100 | 1.3. Другое | 0 | 0 |
| | До 1000 | 500 | | До 5 | 5 |
| | Более 1000 | 1000 | | Более 5 | 10 |
| **2. Число платформ** | | | **2. Не сертифицированные МЗ** | | |
| 2.1. Аппаратные платформы | 1 | 100 | 2.1. АС | 0 | 0 |
| | До 3 | 300 | | До 5 | 4 |
| | Более 3 | 600 | | Более 5 | 8 |
| 2.2. ГОС | Да | 600 | 2.2. СВТ | 0 | 0 |
| | Нет | 0 | | До 5 | 4 |
| 2.3. ЛОС | 1 | 100 | | Более 5 | 8 |
| | 2 | 300 | 2.3. Другое | 0 | 0 |
| | Более 2 | 600 | | До 5 | 2 |
| 2.4. СУБД | 1 | 100 | | Более 5 | 8 |
| | 2 | 300 | **3. Комплексные системы ЗИ** | | |
| | Более 2 | 600 | 3.1. Аттестованные | Да | 20 |
| 2.5. ФПО | 10 | 100 | 3.2. Не аттестованные | Да | 10 |
| | До 100 | 300 | 3.3. Комплексные МЗ | Да | 20 |
| | Более 100 | 600 | | | |
| **3. Характеристики внешнего стыка** | | | **4. Показатели множества угроз** | | |
| 3.1. Физические каналы | 1 | 100 | 1. Глобальные | Да | 40 |
| | 2 | 1000 | | Нет | 0 |
| | Более 3 | 2000 | 2. ЛВС | Да | 40 |
| 3.2. Логические адреса | До 10 | 100 | | Нет | 0 |
| | До 100 | 1000 | 3. АРМ | Да | 20 |
| | Более 100 | 2000 | | Нет | 0 |

Таблица 3

| № п/п | Показатели | Обозначение |
|---|---|---|
| 1. | Показатели сложности ИТКС | G1 |
| 2. | Показатели сложности МЗ | G2 |
| 3. | Показатели множества угроз | G3 |

Таблица 4

| № п/п | Рейтинг (R) | Класс защищенности ИТКС (по РД ФСТЭК России) |
|---|---|---|
| 1. | Более 80 | 1А, 1Б |
| 2. | От 80 до 50 | 1В |
| 3. | От 50 до 30 | 1Г, 1Д |
| 4. | 30 и менее | Отсутствует |

$$R = \frac{\sum_{i=1}^{n} G2_i - \sum_{i=1}^{n} G3_i}{\sum_{i=1}^{n} G1_i};$$

максимальный рейтинг $Rmax = 100$.

Для приведения в соответствие интегрального сравнительного рейтинга с нормативными документами Федеральной службы по техническому и экспортному контролю России используется табл. 4.

Опыт использования интегрального сравнительного рейтинга защищенности показал его полезность для построения и аттестации ИТКС. Структурно-логические и математические модели в области обеспечения информационной безопасности в современных ИТКС применимы в различных условиях и взаимно дополняют друг друга [2]. Наиболее точные оценки и показатели защищенности получаются тогда, когда используется комплекс моделей защиты [3].

**Литература**

1. *Суханов А.В.* Оценки информационных ресурсов и безопасность глобальных информационных систем // Мат-лы V Межрегиональной конференции «Информационная безопасность регионов России – 2007». – Санкт-Петербург, 23–25 октября 2007 г.

2. *Суханов А.В., Николаев А.Ю.* Автоматизация оценки объектов информатизации в соответствии с требованиями руководящих документов «Безопасность информационных технологий» Гостехкомиссии России» // Мат-лы IV Всероссийской конференции «Обеспечение информационной безопасности. Региональные аспекты». – Сочи, 13–17 сентября 2005 г.

3. *Суханов А.В., Андронов А.В., Крылов А.И.* Качественные показатели безопасности информационных ресурсов // «Информация и космос». – 2011. – № 4. – С. 36–39.