МЕТОДИКА ОЦЕНКИ РИСКОВ ДЛЯ АКТИВОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Вашакидзе Гурам Амиранович, магистрант
Паслен Владимир Владимирович, ph.d. технических наук, доцент
Щербов Игорь Леонидович, старший преподаватель
Якушина Анна Евгеньевна, старший преподаватель

Донецкий национальный технический университет, Украина

Участники первенства: Национальное первенство по научной аналитике – «Украина»;

Открытое Европейско-Азиатское первенство по научной аналитике.

Проведен анализ последовательности принятия решения по управлению информационной безопасностью в информационно-телекоммуникационной системе (ИТС) в соответствии с рекомендациями стандарта ISO/IEC 27005 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», ISO/IEC 31010 «Менеджмент риска. Методы оценки риска», Рекомендация МСЭ-Т X.805 «Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами».

Рассмотрена процедура анализа воздействия угроз на свойства информации, подлежащей защите, и на управляемость системы защиты ИТС. Рассмотрены наиболее распространенные методы оценки риска. Предложен порядок дискретной оценки риска для информационно-телекоммуникационной системы на основе экспертных оценок ожидаемого ущерба в случае реализации угроз.

Ключевые слова. *Информационно-телекоммуникационная система, методы оценки риска, методы обеспечения безопасности, алгоритм принятия решений.*

The analysis of the sequence of decision-making information security management of information and telecommunications system (ITS) was made on the base of standard ISO/IEC 27005 "Information Technology. Methods and means of security. Information Security Risk Management " recommendations and ITU-T X.805 "Security architecture for systems providing end-to-end communications" recommendations.

The procedure of analyzing the impact of threats on the properties of the information to be protected, and manageability of the protection of ITS system was considered. The most prevalent methods of risk assessment were considered. The order discrete risk assessment for in information and telecommunications system was proposed on the base of expert estimates of expected damage in case of threats realization.

Keywords. *Information and telecommunication systems, risk assessment, security techniques, decision-making algorithm.*

Постановка задачи

Применение в повседневной жизни как отдельно взятого человека, так и государства в целом, современных информационно-телекоммуникационных технологий позволяет получать все блага достижений современной науки и техники. При этом все значительнее возрастает зависимость процессов жизнедеятельности человека от окружающего его информационного пространства. Данная зависимость приводит к возникновению новых видов угроз – кибернетических преступлений.

Разработка эффективных моделей и методов управления безопасностью информационно-телекоммуникационных систем (ИТС) с целью противодействия кибернетической преступности, является актуальной задачей. Сложность ее выполнения обуславливается такими факторами как:

- необходимость выполнения совокупности технических требований для совместной работы программных продуктов и оборудования различных производителей;
- эффективное использование каналов связи и соблюдение требований электромагнитной совместимости;
- потенциальные угрозы для безопасности ИТС и обрабатываемой в ней информации;
- возможность модернизации;
- себестоимость и др [1].

Безусловно, решение данной задачи должно базироваться на требованиях международных стандартов и рекомендаций. При этом обязательным условием при принятии решения является выполнение требований национального законодательства, регламентирующего данную сферу деятельности.

Анализ состояния проблемы и решение задачи

Учитывая широкий спектр юридических и физических лиц предоставляющих услуги, оборудование и программное обеспечение для информационно-телекоммуникационных систем Международным союзом электросвязи в рекомендации МСЭ-Т X.805 предложена

архитектура защиты для систем, обеспечивающих связь между оконечными устройствами (рис.1). Данная архитектура позволяет произвести детализацию составных частей ИТС, с целью упрощения принятия решения, направленного на эффективное управление, контроль и использования сетевой инфраструктуры, услуг и приложений. Архитектура защиты обеспечивает комплексную, сверху донизу сквозную область сетевой защиты и может применяться к элементам сети, услугам и приложениям, с тем, чтобы обнаруживать, прогнозировать и исправлять уязвимость защиты [2].

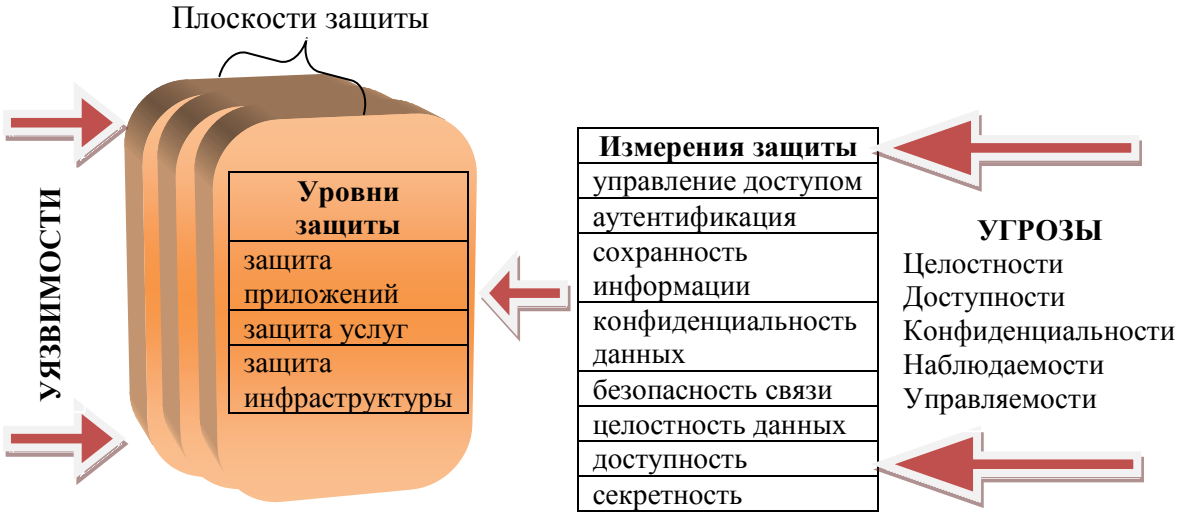


Рис.1. Архитектура защиты систем, обеспечивающих связь между оконечными устройствами.

Принятая архитектура защиты систем, обеспечивающих связь между оконечными устройствами, позволяет более качественно провести оценку риска безопасности ИТС. С этой целью, исходя из рекомендаций международного стандарта ISO/IEC 27005 «Менеджмент риска информационной безопасности», в начальной стадии принятия решения производится учет активов, уязвимость которых может повлиять на степень защищенности ИТС.

Для этого необходимо рассмотреть выделяемые плоскости защиты ИТС:

- управления;
- контроля;
- конечного пользователя.

Следуя рекомендациям МСЭ-Т X.805, для каждой плоскости в соответствии с предназначением, выявляются активы относящиеся к уровню инфраструктуры, предоставляемых услуг, применяемых приложений. Безусловно, к данному процесу должен быть привлечен персонал, имеющий соответсвующую квалификацию и опыт работы.

Так в соответствии с рекомендациями в области стандартизации банка России РС БР ИББС -2.2-2009 установлены следующие требования к привлекаемым экспертам:

- наличие высшего образования;
- опыт работы в данной профессиональной области не менее четырех лет;
- систематическое повышение квалификации;
- способность идентифицировать людей, способных предоставить необходимую информацию;
- обладание навыками делового и управленческого взаимодействия [3].

На следующем этапе определяются угрозы для идентифицированных активов.

Угрозы для ИТС по своей природе подразделяются на природные и техногенные, последние в свою очередь делятся на случайные и умышленные. На данном этапе также определяется источник угроз и «область» действия угрозы, то есть, на какие составные части ИТС может воздействовать данная угроза.

Этап оценки уязвимости активов схематично представлен на рисунке 2.

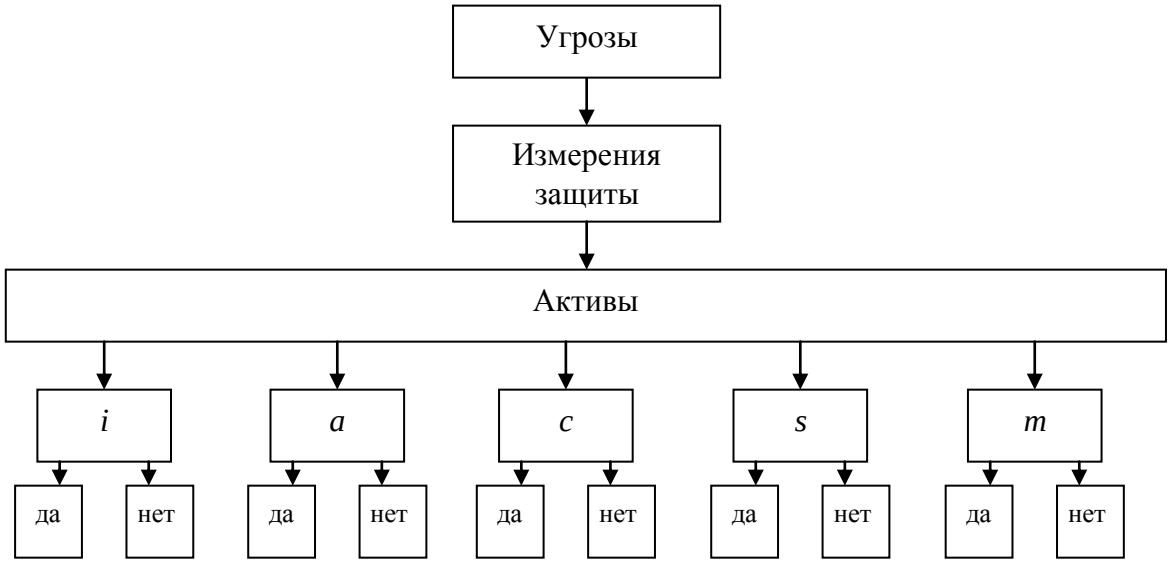


Рис.2. Оценка уязвимости активов от вероятных угроз.

Измерения защиты по своей сути представляют комплекс реализованных мер по защите ИТС. Выделяется восемь основных измерений защиты [2]:

1) управление доступом;
2) аутентификация;
3) сохранность информации;
4) конфиденциальность данных;
5) безопасность связи;

6) целостность данных;

7) доступность;

8) секретность.

В случае успешной реализации угрозы активам может быть нанесен ущерб, который может привести к потере свойств информации или управляемости ИТС:

- целостности *(i)*;
- доступности *(a)*;
- конфиденциальности *(c)*;
- наблюдаемости *(s)*.

Результаты оценки уязвимости активов на примере угроз, которые могут быть реализованы с учетом уязвимости протоколов межсетевого взаимодействия, представлены в таблице 1.

Угрозы для информационной безопасности ИТС Таблица 1

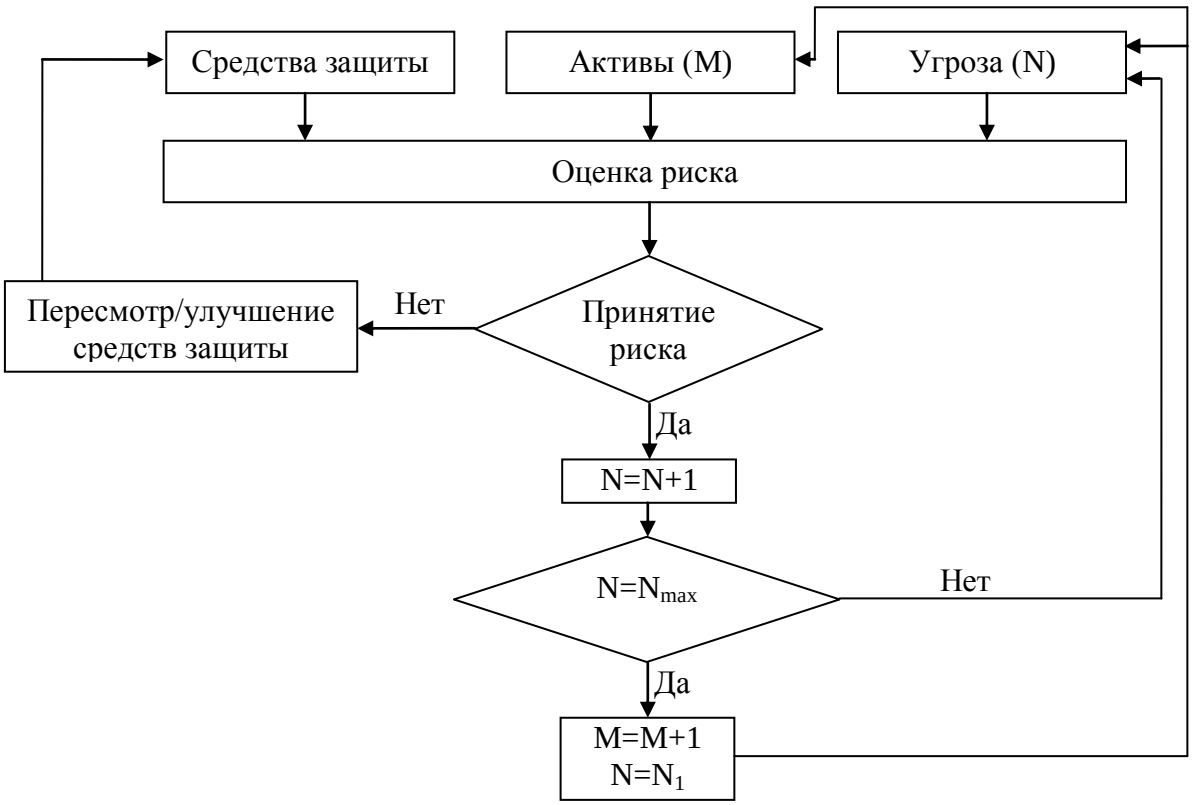
№	Угрозы	конфиденциальность	целостность	доступность	наблюдаемость	весовой коэффициент
1	Анализ протоколов	c_1	i_1	a_1	s_1	p_1
2	Сканирование сетей	c_2	i_2	a_2	s_2	p_2
3	Автоматический подбор паролей	c_3	i_3	a_3	s_3	p_3
4	Spoofing	c_4	i_4	a_4	s_4	p_4
5	Захват сетевых подключений	c_5	i_5	a_5	s_5	p_5
6	Подмена сетевых объектов	c_6	i_6	a_6	s_6	p_6
7	Разнесенный отказ в обслуживании	c_7	i_7	a_7	s_7	p_7
8	Удаленное вторжение	c_8	i_8	a_8	s_8	p_8

Используя полученные данные, можно получить количественную оценку уязвимости конкретного актива от вероятных угроз по следующе формуле:

$$T_k = \frac{c_k + i_k + a_k + s_k}{4} \cdot p_k \qquad (1)$$

Весовой коэффициент p_k определяет чстоту появления данной угрозы относительно совокупности возможных угроз и вычисляется на основе анализа статистических данных или с использованием известных методик [4].

В дальнейшем вопрос принятия риска в упрощенной форме сводится к алгоритму, представленному на рисунке 3.



Примечание: алгоритм повторяется до тех пор, пока M≠Mmax.

Рис.3. Алгоритм принятия риска.

Вывод.

1. Проведенный анализ стандартов и рекомендаций Международной организации по стандартизации, Международной электротехнической комиссии и Международного союза электросвязи, приводит к выводу о необходимости скорейшего внедрения данных документов в повседневную деятельность, с целью повышения защищенности ИТС государства.

2. Рассмотрена процедура анализа воздействия угроз на активы ИТС.

3. Предложен алгоритм оценки риска для информационно-телекоммуникационной системы.

Литература:

1. Воропаєва В. Я., Щербов І.Л. Адаптування інформаційно-телекомунікаційних систем до зовнішніх впливів // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 23 (201). - Донецьк, ДонНТУ, 2012. С - 83-88.

2. Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами (ITU-T X.805 «Security architecture for systems providing end-to-end communications»).

3. Рекомендациями в области стандартизации банка России РС БР ИББС -2.2-2009.

4. Воропаєва В. Я., Щербов І.Л., Е.Д.Хаустова Управління інформаційною безпекою інформаційно-телекомунікаційних систем на основі моделі «plan-do-check-act» // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 25. - Донецьк, ДонНТУ, 2013. С - 104-110.

5. Менеджмент риска- Методы оценки риска (ISO/IEC 31010:2009 «Risk management - Risk assessment techniques»).

6. Информационная технология - Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности (ISO/IEC 27005:2011 «Information technology — Security techniques — Information security risk management»).