КОЛИЧЕСТВЕННАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ АЛЬТЕРНАТИВНЫХ ПРОЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРИ ИНТЕГРАЦИИ

[1]Башлыкова А.А.

[1]Московский технологический университет (МИРЭА), к.т.н., старший преподаватель кафедры корпоративных информационных систем Института информационных технологий, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: bashlykova_a_a_mirea@mail.ru

Основы методологии защиты информации (ЗИ) одинаковы, но принципиальным в КИС, является своевременное выявление предмета защиты и реализация необходимых защитных мер, планирование возможных угроз и мер защиты. Основным критерием должен быть критерий целесообразности и максимальной эффективности предпринимаемых мер, экономических затрат и используемого технического и программного обеспечения. Большинство практических руководств по разработке систем защиты информации посвящены рекомендациям по выбору механизмов и средств обеспечения безопасности, носят неформальный характер и основаны на практическом опыте авторов.

Ключевые слова: корпоративная информационная система, эффективность системы защиты информации, сепарабельность информационных систем.

QUANTITATIVE EVALUATION OF ALTERNATIVE PROJECT OF PROTECTION DATA OF INTEGRATION OF INFORMATION SYSTEM

[1]Bashlykova A.A.

[1]Moscow University of Technology (MIREA), 119454, Russia, Moscow, Vernadsky prospect, 78, e-mail: bashlykova_a_a_mirea@mail.ru

The basics of methodology of information protection (IP) is the same, but fundamental in the keys, is the timely identification of the subject of protection and the implementation of necessary protective measures, planning for possible threats and protection measures. The main criterion should be the criterion of expediency and efficiency of the measures taken, the economic costs and used hardware and software. The most practical guidance on the development of systems of information security is devoted to recommendations for the selection of mechanisms and means to ensure security, are informal and are based on the practical experience of the authors.

Key words: corporate information system, the effectiveness of information security systems, information systems separability.

Предисловие

Осуществление безопасности функционирования объекта (корпоративной информационной системы, КИС) реализуется посредством системы защиты, под которой принято понимать комплекс мер и средств, направленных на выявление, отражение и ликвидацию различных видов угроз функционирования объекта. При этом совершенно очевидно, что каждый объект будет иметь свою специфику, которая должна найти свое отражение в системе защиты.

Масштабы развития КИС и сферы их применения стали таковы, что наряду с проблемами надежности и устойчивости функционирования КИС возникает проблема обеспечения безопасности обрабатываемой ими информации.

Частной задачей построения единой концепции ЗИ является задача формализации процессов оценивания эффективности защиты системы обработки информации и выбора механизмов безопасности для построения системы защиты информации.

В соответствии с изложенным, данная статья нацелена на описание наиболее подходящих решений задачи количественной оценки показателей эффективности альтернативных проектов защиты КИС и на

основе полученного результата - формулирование методики выбора механизмов обеспечения безопасности КИС. Данное направление потребует дальнейшего рассмотрения.

Информационную систему (ИС) можно представить тройным значением IS ={B,M,K}, где B –начальная формальная база данных (БД), M - матрица прав доступа к БД и K – некоторое множество команд изменения прав доступа в M.

При причислении ИС к вхождению в корпоративную информационную систему (КИС) предполагается наличия свойства сепарабельности каждой ИС в КИС, с возможностью чтения субъектами одной ИС собственных данных другой ИС, входящих в КИС, без модификации данных. При внедрении на компоненты и в компьютерную сеть КИС проекта защиты информации (ЗИ) , происходит интеграция системы защиты информации (СЗИ) в КИС. Цель внедрения СЗИ: исключение несанкционированного манипулирования субъектами отдельных ИС, собственными данными в ИС; сохранение вложенности подчиненных объектов (в зависимости от политики безопасности (ПБ)); сохранение целостности данных, ставших общими и представленных только в конкретной ИС. Несанкционированная модификация несобственных данных исключается условием сепарабельности ИС в КИС, интероперабельности данных и открытости интерфейсов.

Как показывает анализ, большинство современных КИС в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) ИС и отдельных ПК.

Под системой защиты информации (СЗИ) в КИС понимается защита [1]: – во всех структурных элементах КИС;

– на всех участках и технологических маршрутах обработки информации;

– при всех режимах функционирования КИС;

– на всех этапах жизненного цикла КИС;

– с учетом взаимодействия КИС с внешней средой.

В дальнейшем, в статье, предполагается, что речь пойдет о СЗИ, в которых работают механизмы и средства со свидетельствами и документами о прохождении сертификации.

Современные публикации по теории защиты информации в КИС, в основной своей массе посвящены рассмотрению верхних уровней иерархии анализа СЗИ. Из анализа стандартов и современной литературы по проблемам безопасности и защиты информации для переноса решений в КИС не вполне ясно, как:

– оценить эффективность выполнения целевой задачи СЗИ при воздействии дестабилизирующих факторов (ДФ) на КИС;

– определить уровень потенциального ущерба от воздействия того или иного ДФ на КИС;

– исходя из допустимого уровня потенциального ущерба, который может быть нанесен КИС в результате атак ДФ, осуществить оценку эффективности СЗИ, как средства поддержки и реализации ПБ КИС.

Следует отметить, что задача оценивания эффективности СЗИ является достаточно сложной и на сегодняшний день остается нерешённой для КИС. Возникающие при её решении трудности связаны с необходимостью учёта неопределённости в описании возможных КИС.

Поиск путей решения проблемы привёл к пяти различным методам получения оценок качества СЗИ [2,3]:

1. Проведение сертификационных испытаний.
2. Привлечение специалистов.
3. Использование автоматизированных инструментальных средств оценки рисков (@RISK, ALRAM, CRAMM, LAVA и др.);
4. Использование средств тестирования защищённости АС (KSA, ISS, SATAN,COPS, и др.);

На данный момент при работах по обеспечению ЗИ в КИС, наибольшее внимание уделяется ДФ, воздействующим без подключения к линиям связи: перехват ПЭМИН, наводок в цепях питания и т.п. и ДФ, на вероятность успешной реализации которых можно повлиять рядом организационных мероприятий: кражи, хищения, диверсии, внедрение агентов и т.д.

С развитием общедоступных сетей связи и подключением к ним КИС наибольший интерес вызывает класс ДФ, воздействующих через общедоступные линии связи. В современных КИС используются не специализированное, а общедоступное программное обеспечение, что увеличивает вероятность появления ДФ, использующих, в том или ином виде, ПО КИС, особенно важно это в отношении сетевого и системно-сетевого ПО.

Самооценка выполняется организацией с целью оценки собственной СЗИ КИС, или в отношении конкретного элемента СЗИ.

Автоматизированные инструментальные средства оценки рисков, содержащие, в сущности, простейшие модели СЗИ, пользовались популярностью сравнительно короткое время в начале 90-х годов. Возникающие при их применении сложности связаны, во-первых, с подготовкой исходных данных для оценивания защищённости объектов, и, во-вторых, с необходимостью постоянного обновления базы данных по известным ДФ и механизмам безопасности.

На рисунке 1. показаны роли процесса оценки защиты КИС и основные функции, выполняемые ролями.
Использование средств тестирования защищённости СОИ, моделирующих ИВ на объекты АСУ, может рассматриваться только как дополнительная возможность получения комплексной, сбалансированной оценки качества СЗИ, в связи с тем, что:

– бессистемность проводимых проверок не позволяет выработать требования и рекомендации по ОБИ на основе результатов тестирования;

– недостатки документации на средства тестирования и отчетных документов по результатам проверок существенно снижают их практическую ценность[5].

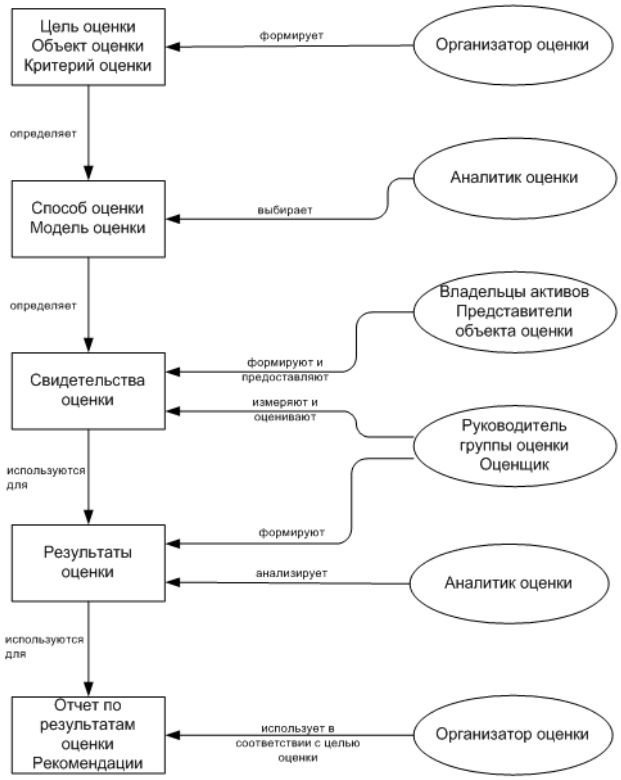

Рис. 1. Роли процесса оценки КИС и их функции

Из анализа относительно полного множества ДФ при построении модели воздействия ДФ на КИС наибольший интерес вызывают ДФ - искусственные по происхождению, преднамеренные по характеру возникновения, воздействующие с помощью программных средств, осуществляемые с подключением к линиям связи и на успешное осуществление которых повлиять невозможно.

Уровень предотвращенного потенциального ущерба КИС в результате атак ДФ может быть выбран в качестве одного из частных показателей эффективности СЗИ КИС.

Другая интерпретация уровня предотвращенного ущерба это уровень защищенности КИС.

Данный частный показатель непосредственно влияет на эффективность системы защиты информации и физически выражает положительный эффект или выгоду – L.

Другим частным показателем эффективности защиты КИС является показатель, который косвенно влияет на эффективность защиты информации - затраты на реализацию системы защиты информации (потери), отрицательный эффект – R.

Т.е. обобщенный показатель эффективности имеет векторный вид:

$$\omega = [L\ R]$$

Разработка критерия эффективности защиты КИС для векторного показателя существенно усложняется по сравнению со случаем скалярного показателя.

Причина этого усложнения - наличие между показателями зависимости по предпочтению. Существенно упростит решение задачи разработки критерия эффективности защиты системы обработки информации переход к единственной целевой функции показателей - целевой функции безопасности КИС.

Критерий эффективности защиты КИС в этом случае представляет собой условие, которому должна удовлетворять целевая функция $\varphi(\omega)$, где $\omega = [L\ R]$.

Одним из основных способов построения целевой функции для векторного показателя эффективности является субъективное свертывание с выделением "главного" показателя.

На практике целевой задачей СЗИ КИС является предотвращение потенциального ущерба от атак ДФ на элементы КИС при этом допустимые затраты на реализацию СЗИ ограничены, поэтому в качестве обобщенного критерия эффективности СЗИ можно предложить следующий:

$$\{ L = max, R \le R_{доп} \}$$

Значение предотвращенного ущерба – L, должно быть максимальным при ограниченных затратах на реализацию системы защиты КИС.

Наибольшее влияние на расчет предполагается, что оказывают значения следующих параметров:

- время мониторинга безопасности КИС (время обнаружения атаки, регламентируется согласно принятой ПБ) - T_m;
- время восстановления элементов КИС - $T_в$ (почти во всех КИС заданы жесткие ограничения);
- интенсивности атак ДФ на элементы КИС;
- прочностей механизмов безопасности элементов КИС - P_D.

Положение осложнено тем, что время интенсивности атак ДФ на КИС не контролируемо.

Таким образом, в качестве параметров для анализа особенностей целевой функции могут быть выбраны прочности механизмов безопасности.

Однако неопределенность структуры КИС позволяет оценить лишь область значений целевой функции, а также качественные изменения целевой функции при варьировании параметров.

Из анализа физического смысла целевой функции следует, что для определения области значения необходимо определить значения целевой функции в следующих двух случаях:

Прочности всех механизмов безопасности равны 0 P_D= {0,...,0} , что соответствует отсутствию защиты у всех элементов КИС.

$$\lim \varphi = 0$$
$$P_D = \{0,\ldots 0\}$$

Прочности всех механизмов безопасности равны 1 P_D ={1,...,1} –абсолютно защищенная КИС.

$$\lim \varphi = \underline{L'}$$
$$P_D = \{1,\ldots 1\}$$

Таким образом, область значений целевой функции равна [0,L´].

Анализ качественных изменений целевой функции от прочностей механизмов безопасности можно провести лишь для конкретных элементов КИС.

Тогда задача оценки альтернативных проектов защиты КИС заключается в выборе таких значений $P_{Dnm}i$ (1), чтобы значение предотвращенного ущерба было максимальным при ограниченных затратах на построение проекта защиты КИС:

$$\left.\begin{array}{l} \max \mathbf{L}(P_{D_{nmi}}) \\ n=\overline{1,N}; m=\overline{1,M}; i=\overline{1,2^K-1} \\ R \le R_{доп} \end{array}\right\} \quad (1)$$

Максиминный критерий Вальда.

Для решения этой задачи целесообразно использовать алгоритмы оптимизации, использующие методы прямого поиска. В частности, для решения рассматриваемой задачи хорошие результаты, с точки зрения быстродействия и точности вычислений, дает использование метода прямого поиска Хука и Дживса [4].

Суть данного метода заключается в поиске максимума многомерной функции с помощью многошаговой процедуры, на каждом шаге которой изменяется только одна переменная, тогда как другие остаются постоянными, пока не будет достигнут максимум. При этом используются априорные сведения и в то же время отвергается устаревшая информация.

Во-вторых, может потребоваться остановится между линией поведения «рассчитывай на худшее» и линией «рассчитывай на лучшее».

В этом случае оптимальным решением будет то, для которого окажется максимальным показатель Г (критерий пессимизма-оптимизма Гурвица,2):

$$\Gamma = k \min \{ L\ P_{Dnm}{}^i \} + k \max \{ L\ P_{Dnm}{}^i \} , (2)$$

где *k*- коэффициент, выбираемый в интервале [0 , 1] (при *k*=0 –линия поведения в расчете на лучшее, при *k*=1 – линия поведения в расчете на худшее, 3).

$$\Gamma = 1/2 \min \{ L\ P_{Dnm}{}^i \} + 1/2 \max \{ L\ P_{Dnm}{}^i \} (3)$$

В-третьих, может иметь место требование в любых условиях избежать большого риска.

Здесь оптимальным решением будет то, для которого риск, максимальный при различных вариантах обстановки, окажется минимальным (минимаксный критерий Сэвиджа).

Анализ критериев показал, что их использование необходимо проводить в соответствии с системой исходных данных.

Как показывает опыт российских предприятий за 2011 год кортеж приоритетности использования оценку эффективности СЗИ КИС можно разбить на три неравные группы:

15% от общего числа будут составлять наиболее значимые предприятия (филиалы); 35% - средние предприятия и их филиалы; 50% - менее критичные с точки зрения потерь филиалы предприятий. Для

первой группы наиболее целесообразно использовать критерий Вальда, для второй- Гурвица, для третьей –Сэвиджа.

Оценивается проект СЗИ КИС предприятия не связанного:

- с банковской системой РФ и банковской сферой.
- с защитой государственной тайны.

Таким образом, алгоритм рациональной оценки по перечисленным критериям альтернативных проектов (рационального выбора механизмов безопасности для построения) защиты КИС будет следующим:

1. сформировать полный перечень доступных механизмов безопасности элементов КИС $D=\{D_1,\dots D_k,\dots,D_K\}$;
2. определить прочности механизмов безопасности $P_D=\{P_{D1},\dots, P_{Dk}\}$.
3. определить полную стоимость построения каждого проекта защиты КИС

$$\overline{Rj},\ j=1,J;$$

4. определить описанными выше методами наилучшие параметры построения проекта защиты КИС

$$X_{best}=\{P_{Dnm}i_{best}\},m=1,M;\ n=1,N;\ i=1,2^K-1;$$

для которых выполняется $\max L\{P_{Dnm}i\}$, $\min L\{P_{Dnm}i\}$, или
$1/2 \min\{L P_{Dnm}^i\} + 1/2 \max\{L P_{Dnm}^i\}$ в зависимости от выбранного критерия ;

5. определить проекты построения защиты КИС с параметрами

$$X_{best}:\overline{Sj},\ j=1,J;$$

6. осуществить выбор вариантов построения КСЗИ КИС, которые удовлетворяют требованию по стоимости

$$Rj \le R,\ j=1,J;$$

7. если в процессе решения задачи выбора механизмов безопасности требованию по стоимости удовлетворяют несколько проектов построения защиты КИС, то осуществить выбор альтернативного проекта построения защиты КИС по критерию

$$\psi = \frac{L(Xmax)}{Rj}$$

8. если в процессе оценки альтернативных проектов (решения задачи выбора механизмов безопасности) защиты системы обработки информации требованию по стоимости не удовлетворяет ни один из вариантов построения защиты КИС с параметрами X_{best} , то назначаются уступки по стоимости системы защиты информации.

Например, проверка проведения оценки эффективности СЗИ КИС показала (таблица 1, представленный фрагмент), что если были выбраны 4 элемента СЗИ КИС, 7 наиболее вероятных ДФ, и 17 механизмов безопасности, то число различных альтернативных проектов защиты КИС составит 216. При этом среди 216 различных вариантов проекта – количественно можно выбрать меньшее число претендентов, а из них – один проект, который получит максимально удовлетворит требованиям.

Фрагмент таблицы 1. Показатели проектов защиты КИС, с которыми работал программный инструментарий, по указанным этапам методики оценки по перечисленным критериям альтернативных проектов защиты КИС

Результаты экспериментальной проверки предлагаемой методики оценки по выбранным критериям	1	2	3	4
	R	L	*f*	Оптимальный проект защиты КИС
S1 (D1,D2,D5,D8,D10, D13,D15)	10120	0,54	5,33597E-05	
S2 (D1,D3,D5,D8,D10, D13,D15)	7980	0,61	7,644111E-05	по критерию Гурвица
S3 (D1,D4,D5,D8,D10, D13,D15)	8670	0,5	5,76701E-05	
…..				
S8 (D1,D3,D7,D8,D10, D13,D15)	8280	0,34	4,10628E-05	по критерию Сэвиджа
….				
S21 (D1, D4, D5, D8, D11, D13,D15)	7970	0,87	0,000109159	по критерию Вальда
….				
S27(D1,D4, D7, D8, D11, D13, D15);	8270	0,34	4,11125E-05	по критерию Сэвиджа
….				
S215(D1, D3, D7, D9, D12, D14, D16)	16080	0,79	4,91294E-05	
S216(D1, D4, D7, D9, D12, D14, 016)	16770	0,88	5,24747E-05	

Полная таблица включает в себя все 216 строчек, каждая из строчек - это проект защиты КИС S , состоящий из механизмов безопасности D_n и соответствующие проекту значения стоимости построения - R, математическое ожидание потенциального ущерба- L, и f – значение целевой функции.

Защищенность информации не является абсолютной характеристикой КИС и может рассматриваться только относительно некоторой среды, в которой фиксируются определенные угрозы (СЗИ). Потребность в применении универсального метода оценки эффективности СЗИ КИС есть у государственных учреждений и организаций, для которых, в силу их специфики, вопросы организации

безопасности и защиты информации стоят наиболее остро определили широкое использование сертификационных испытаний, проводимых в соответствии с Руководящими документами ФСТЭК России.

Заключение.

Конечной целью защиты КИС и циркулирующей в ней информации является предотвращение или минимизация наносимого субъектам информационных отношений ущерба посредством воздействия на компоненты КИС дестабилизирующих факторов. Отсюда ясна целевая задача системы защиты КИС – минимизация потенциального ущерба.

Анализ критериев эффективности СЗИ нескольких КИС показал, что их использование необходимо проводить в соответствии с системой исходных данных, и при изменении/модернизации/ интеграции КИС и самой СЗИ – результатам последней оценки не доверять и проводить повторно, при новом составе КИС.

Описанные подходы к оценке эффективности СЗИ КИС имеют свои недостатки:

– материальные и временные затраты на проведение сертификационных испытаний;

– невозможность применения к исследованию защищенности микрокомпьютеров и локальных сетей;

– учет издержек на обеспечение безопасности толь на последнем этапе;

– полученные оценки (на соответствие одному из классов защищенности) отражают только количественный аспект и не определено, как учитывать качественный, и переводить в количественные значения;

– трудность оценки в динамически изменяемой КИС с течением времени.

Анализ качественных изменений целевой функции от P_D можно провести лишь для конкретных элементов КИС. Целевая задача СЗИ КИС – минимизация потенциального ущерба, и особенно важно при интеграции, т.к. этот процесс и сам несет вероятность ущерба. В данной статье представлено описание наиболее подходящих решений задачи количественной оценки показателей эффективности альтернативных проектов защиты системы КИС и сформулирована методика выбора механизмов обеспечения безопасности КИС, – которыми смогут воспользоваться специалисты при задании руководства для оценки.

Оценка должна производится группой экспертов (рис.1.), а итог должен быть перепроверен руководством или сравниваться в результатами оценки приглашенных экспертов по договору с специализированной организацией.

Список литературы

1. Национальный стандарт РФ ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения, 01.09.2014г.
2. Грездов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы: монография / Г. Г. Грездов. – К.: ГУИКТ, 2009. – 32 с.
3. Парахин В.П., Смирнов В.В. Оценка качества функционирования СОИ при воздействии угроз. Тезисы ежегодной научно-практической конференции "Методы и технические средства обеспечения безопасности информации", - СПб. 2009.
4. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств (по материалам интернет-изданий за 2008-2010 гг.) [электронный ресурс] http://www.securitylab.ru/analytics/398184.php
5. Петренко С.А. Александрович Г.Я, Нестеров С.А, Автоматизация оценки информационных рисков компании// Защита информации. Конфидент.2003,№2, с.78-81.

References

1. Russian Federation National Standard GOST R 51583-2014 Information Security. The order of creation of automated systems in the protected design. General provisions 01.09.2014g.
2. Grezdov G.G. The modified method of solving the problem of the formation of an effective integrated protection system information of the automated system: monograph / GG Grezdov. - K .: SUICT, 2009. - 32 p.
3. Parahin V.P., Smirnov V.V. Evaluation of the quality SDI operation when subjected to threats. Abstracts of the annual scientific and practical conference "Methods and technical tools of information security", - SPb. 2009.
4. Review of Information Security Incident ACS foreign countries (based on online publications for 2008-2010.) [Electronic resource] http://www.securitylab.ru/analytics/398184.php
5. Petrenko S.A., Aleksandrovich G.YA., Nesterov S.A. Automation evaluation of information risks // Information Security. Konfident.2003, №2, s.78-81.