УДК 004.056

А.А. Замула[1], А.В. Северинов[2], М.А. Корниенко[3]

[1] *Харьковский национальный университет имени В.Н. Каразина, Харьков*
[2] *Харьковский университет Воздушных Сил имени И. Кожедуба, Харьков*
[3] *Харьковский национальный университет радиоэлектроники, Харьков*

АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В данной статье рассмотрены модели оценки рисков информационной безопасности для анализа информационных систем и построения эффектных систем защиты информации. Проведен анализ моделей на основе матрицы системы управления информационной безопасностью, включая качественные и количественные шкалы и на базе теории нечетких множеств.

Ключевые слова: *оценка рисков информационной безопасности, система управления информационной безопасностью, информационная безопасность, нечеткая логика, нечеткие когнитивные карты.*

Введение

Интенсивное развитие компьютерных систем и информационных технологий способствовало их внедрению во все сферы жизни современного общества. Вместе с тем переход от ведения дел с помощью бумажных документов к электронному документообороту, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным, появлению новых уязвимостей в информационных системах и компьютерных сетях. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и компаний, работающих в сфере электронного бизнеса.

Общая постановка проблемы. В современном обществе методы воздействия на конкурентов переходят от физического воздействия к интеллектуальному. При этом используются новейшие способы и средства несанкционированного получения информации. Именно поэтому актуальным является необходимость оценки рисков информационной безопасности для построения эффективных систем защиты информации (СЗИ).

Основой модели оценки рисков является построение метода, который позволит как можно точно описать существующую информационную систему (ИС) с учетом ее ресурсов и уязвимостей. Существует множество методов оценки рисков. В статье рассмотрены методы на основе построения «Матрицы СУИБ» и на базе нечетких множеств (нечетких когнитивных карт).

Целью статьи является исследование и анализ моделей оценки рисков информационной безопасности для построения эффективной системы защиты информации.

Модель на основе построения «Матрицы СУИБ»

Данная модель предназначена для исследования уже существующей информационной системы и СЗИ с целью модернизации системы защиты и повышения защищенности информационных ресурсов.

Для исследования информационной системы предложен метод, основанный на построении системы управления информационной безопасностью (СУИБ). При этом СУИБ может представлять собой базу знаний о данной информационной системе и СЗИ. Данные, полученные в результате анализа информационной системы, позволят определить оптимальные меры по обеспечению защиты информации.

Рассмотрим один из способов построения СУИБ на основе «Матрицы СУИБ» (далее Матрица), изображенной на рис. 1 [1]. Матрица позволяет логически объединить составляющие блоков "Основы" (Объекты), "Направления" и "Этапы" по принципу: каждый с каждым. Система защиты информации лишь тогда станет системой, когда будут установлены логические связи между всеми ее составляющими [1]. Известно, что основой или составными частями практически любой системы (в том числе и системы защиты информации) являются:

- законодательная, нормативно-правовая и научная база;
- структура и задачи органов (подразделений), обеспечивающих безопасность информационных ресурсов;
- организационно-технические, режимные меры и методы (политика информационной безопасности);
- программно-технические способы и средства.

Направления защиты формируются исходя из особенностей ИС как объекта защиты, а также типовой структуры ИС и исторически сложившихся видов работ по защите информации.

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис. 1. Построение матрицы СУИБ

Этапы - это последовательность шагов построения СЗИ, которые необходимо пройти в равной степени для всех и каждого в отдельности Направлений (с учетом всех основ). Проведенный анализ данной модели позволяет выделить этапы, представленные на рис. 1. Элементы матрицы имеют соответствующую нумерацию, где:

- первое знакоместо (X00) соответствует номерам составляющих блока “Этапы”,
- второе знакоместо (0X0) соответствует номерам составляющих блока “Направления”,
- третье знакоместо (00X) соответствует номерам составляющих блока “Основы” [1].

Каждый элемент подразумевает связь трех составляющих и представляет собой требование, которое должно быть выполнено. Например, элемент матрицы «111» может иметь следующее описание: «Изложение в законодательных, нормативных и методических документах вопросов, определяющих перечень сведений, имеющихся на объектах ИС, которые подлежат защите, и порядок определения таких сведений» [4]. Таким образом, каждый элемент матрицы описывает: какие требование должны быть выполнены на определенном этапе создания СЗИ и на каких основаниях.

Прежде всего, для оценки состояния СЗИ необходимо определить, какие активы и ресурсы подлежат защите, и какие угрозы могут быть осуществлены в отношении данных активов. Матрица предполагает определение уровня значимости актива по отношению к значимости других активов по шкале 1-5. Аналогичным способом определяется частота осуществления угроз (рис. 2).

Возможный ущерб рассчитывается как произведение значения убытка на частоту появления угрозы. Таким образом, можно построить таблицу оценки рисков (рис. 3), где максимальное значение определяет, какой актив более всего подвержен угрозам и влечет за собой дальнейшие убытки и утрату информации. Следовательно, для этого актива необходимо применить меры защиты.

На основе данной матрицы можно оценить не только риски информационной безопасности в соответствии с определенными шкалами, но и степень выполнения требований по обеспечению информационной безопасности в уже существующей СЗИ или на стадии ее разработки.

В данном случае применяются наиболее распространенные методики на основе качественных и количественных оценок.

Качественная шкала может иметь несколько градаций, например: низкий, средний и высокий уровни. Оценка производится экспертом с учетом ряда объективных факторов.

Загроза	Частота	Актив	Збиток	Оцінка ризику
DDoS-атака	5	IP-пакети	3	15
DDoS-атака	5	Трафік	4	20
Взлом WEP-ключів	1	WEP-ключі	3	3
Взлом WEP-ключів	1	Паролі	2	2
Всі загрози	5	Всі активи	5	25
Імперсоналізація	2	ARP-запис	3	6
Імперсоналізація	2	IP-пакети	3	6
Імперсоналізація	2	WEP-ключі	3	6

Рис. 2. Построение таблицы значимости активов и частоты реализации угроз

	Актив						
	ARP-запис	IP-пакети	WEP-ключі	Всі активи	Паролі	Трафік	Общие итоги
Загроза	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику
DDoS-атака		15				20	35
Взлом WEP-ключів			3		2		5
Всі загрози				25			25
Імперсоналізація	6	6	6	10	4	8	40
Підміна ARP-записів	9						9
Фальсифікація IP-пакетів		12					12
Общие итоги	15	33	9	35	6	28	126

Рис. 3. Оценка рисков информационной системы (беспроводная сеть)

Если применяются качественные методы, возможные риски нарушения ИБ должны быть ранжированы по степени их опасности с учетом таких факторов, как цена возможных потерь, уровень угрозы и уязвимости.

Риски могут быть оценены с помощью количественных шкал. Это даст возможность упростить анализ существующих угроз в ИС и выбор мер защиты.

Однако в этом случае предъявляются более высокие требования к шкалам измерения исходных данных.

Для проведения оценки эффективности выбранных мер защиты заполняется таблица (рис. 4), которая имеет ряд параметров [5].

Параметры таблицы:

- «Коэффициент важности» - значимость одной из Основ Матрицы по отношению к другим в рамках одного Этапа.
- «Профиль безопасности требуемый» - это граница, которую системе необходимо достичь для обеспечения защиты информации. Принимает значения от 0,8 до 1 (или же выполнение 80-100%).
- «Профиль безопасности достигнутый» - это показатель, который характеризует на сколько процентов был выполнен профиль безопасности по отношению к требуемому профилю безопасности. Принимает значения от 0 до 1 (может превышать значение «Профиль безопасности требуемый», если это требование выполнено более качественно, нежели было достаточно).
- «Сравнение профилей» - показатель, который принимает значения «0» или «1». Значение «1» принимается в том случае, если «Достигнутый показатель безопасности» больше или равен «Требуемому показателю безопасности», в противном случае - устанавливается «0».
- «Степень выполнения групп требований» - качественная оценка выполнения требований по одному этапу. Показатель рассчитывается как среднее арифметическое показателей «Степень выполнения требования» по одному этапу.
- «Качественная оценка» - оценка выполнения требований по всем этапам.
- «Количественная оценка» - оценка количества выполненных по отношению к общему количеству выдвинутых требований.

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qд x aj	Сравнение профилей	Степень выполнения групп	Качественная оценка	Количественная оценка
	m	№	a_j	Qmp	Qд	Qдaj	Sпр	Qгруп	Q	S
1	1	131	0,5	0,8	0,7	0,35	0	0,68		
	2	132	0,2	0,8	0,8	0,16	1			
	3	133	0,15	0,8	0,5	0,08	0			
	4	134	0,15	0,8	0,6	0,09	0			
2	5	231	0,25	0,8	0,5	0,13	0	0,73		
	6	232	0,25	0,8	0,8	0,2	1			
	7	233	0,25	0,8	0,8	0,2	1			
	8	234	0,25	0,8	0,8	0,2	1			
3	9	331	0,25	0,8	0,6	0,15	0	0,60		
	10	332	0,25	0,8	0,6	0,15	0			
	11	333	0,25	0,8	0,6	0,15	0			
	12	334	0,25	0,8	0,6	0,15	0			
4	13	431	0,25	0,8	0,8	0,2	1	0,70	0,67	0,39
	14	432	0,25	0,8	0,8	0,2	1			
	15	433	0,25	0,8	0,6	0,15	0			
	16	434	0,25	0,8	0,6	0,15	0			
5	17	531	0,25	0,8	0,6	0,15	0	0,65		
	18	532	0,25	0,8	0,6	0,15	0			
	19	533	0,25	0,8	0,6	0,15	0			
	20	534	0,25	0,8	0,8	0,2	1			
6	21	631	0,25	0,8	0,5	0,13	0	0,65		
	22	632	0,25	0,8	0,5	0,13	0			
	23	633	0,25	0,8	0,8	0,2	1			
	24	634	0,25	0,8	0,8	0,2	1			
7	25	741	0,25	0,8	0,8	0,2	1	0,80		
	26	742	0,25	0,8	0,8	0,2	1			
	27	743	0,25	0,8	0,8	0,2	1			
	28	744	0,25	0,8	0,8	0,2	1			

Рис. 4. Оценка эффективности СЗИ

Итогом заполнения данных полей таблицы являются графики (рис. 5 – 7), которые показывают степень выполнения мер защиты информации.

Рис. 5. Оценка достигнутого профиля защиты

Например, рис. 5 иллюстрирует то, что было достигнуто выполнение всего 11 мер защиты из 28. Остальные же требования были выполнены частично (рис. 6).

Графики на рис. 6 показывают: насколько качественно были выполнены требования по обеспечению защиты информации в сравнении с требуемым уровнем. Рис. 7 демонстрирует, насколько качественно и полно были выполнены все этапы по созданию СЗИ и какие этапы требуют усовершенствования (показатель «1» является выполнением требования на 100 %) [5].

Рис. 6. Сравнение профилей защиты

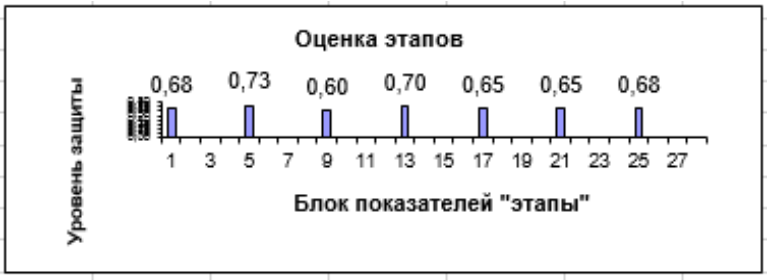

Рис. 7. Оценка качества выполнения этапов разработки и внедрения СЗИ

Анализ данной модели оценки рисков информационной безопасности показал, что модель, основанная на построении «Матрицы СУИБ», позволяет оценить важность и уязвимость ресурсов информационной системы. Преимуществом модели является полнота описания ИС, ее ресурсов и уязвимостей. Оценка рисков информационной безопасности позволяет выделить наиболее важные или уязвимые ресурсы, в результате чего, следует выбрать необходимые меры и средства по защите данных ресурсов. Также положительным является возможность оценки существующей системы защиты информации, и определение полноты мер и требований по обеспечению защиты информации.

Недостатком метода является наличие субъективного мнения по определению важности активов и частоте реализации угроз.

Модель оценки рисков информационной безопасности на основе нечетких множеств

Модель расчета рисков ИБ на основе нечетких множеств строится с использованием нечетких когнитивных карт (НКК). Нечеткие когнитивные карты представляют собой простой граф из узлов и взвешенных дуг, где узлы – концепты предметной области (например: множество нарушителей, множество способов преодоления системы защиты), а дуги причинно-следственные связи между ними (например: вероятность наличия определенного вида нарушителей, вероятность реализации атаки и др.).

В общем случае при расчете риска используют соотношение:

$$R_{ij} = P_i^u \cdot P_{ij}^v \cdot A_j,$$

где R_{ij} – риск j-го ресурса по отношению к i-й угрозе;

P_i^u – вероятность i-й угрозы;

P_{ij}^v – уязвимость защиты j-го ресурса по отношению к i-й угрозе;

A_j – ценность j-го ресурса.

Вес связей в нечетких когнитивных картах задается в нечетком виде: с помощью лингвистических терм или интервальных оценок [3].

С помощью НКК (рис. 8) вычисляется полный эффект влияния совокупности угроз на некоторый информационный ресурс системы или же на множество ресурсов ИС.

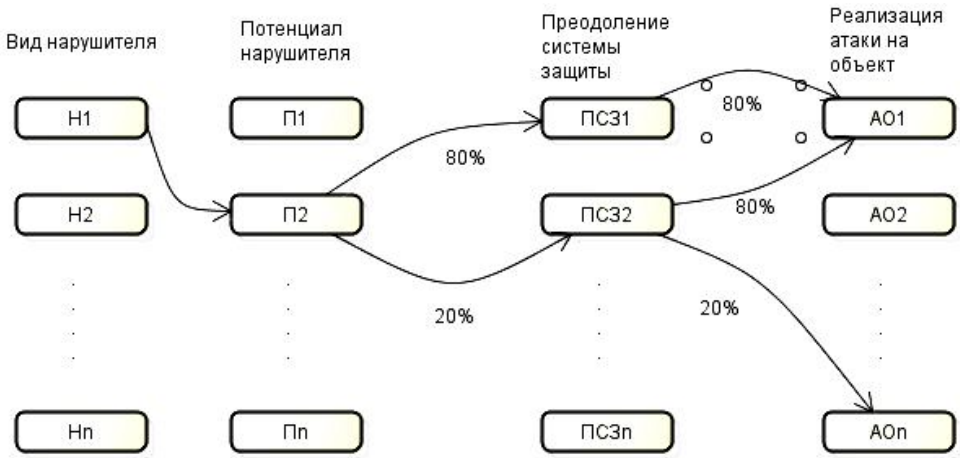

Рис. 8. Нечеткая когнитивная карта с дугами, имеющими переходы по бальной шкале

На основе полученных данных затем вычисляется риск [2]. В работе предлагаются модели с лингвистической и балльной шкалами для оценки уровня защищенности ИС на основании экспертных оценок (эталонных значений) и результатов опроса пользователей, осуществляющих оценку принятых в ИС мер защиты.

Нечеткая модель с лингвистической шкалой реализуется по результатам опроса пользователей системы, согласно предварительно составленного экспертами запроса [3].

Пример одного из листов опроса экспертов приведен на рис. 9 [6].

Модель предполагает, что группа из N пользователей отвечает на n вопросов (n-компонентный экспертный запрос) соответственно составленной экспертом по нечеткой шкале (Да, Нет, Затрудняюсь ответить). По ответам пользователей формируется нечеткое число, которому ставится в соответствие одно из эталонных. Суммарную оценку безопасности ИС определяют с учетом заранее вычисленных коэффициентов важности.

В нечеткой модели с балльной шкалой пользователь также отвечает на предварительно ранжированные вопросы (компоненты экспертного запроса) по составленной экспертом N-балльной шкале. Диапазон шкалы может варьироваться в зависимости от сложности оценки угрозы и при этом определяется показатель уровня защищенности по соответствующему логическому выражению [3].

Преимущество модели оценки рисков информационной безопасности на основе нечетких множеств состоит в применении аппарата нечеткой логики, т.к. процесс защиты информации не всегда можно описать формально, особенно, это касается поведения персонала.

Опрос эксперта №1 о наличии нарушителей

Тип источника угрозы	Вопрос эксперту	Ответы эксперта					
		Да		Нет		Затрудняюсь ответить	
		Метка ответа	Коэф-фициент	Метка ответа	Коэф-фициент	Метка ответа	Коэффи-циент
Внутренние нарушители (администраторы, сотрудники служб ИБ, прикладные и системные программисты, непосредственные пользователи и операторы беспроводной сети)	Требуется ли от кандидата при приеме на работу рекомендации с прежних мест работы?		0	+	1		0,5
	Проводится ли при приеме на работу тестирование личных качеств, а также точности и полноты биографических данных?	+	0		1		0,5
	Разработаны ли должностные инструкции для сотрудников?	+	0		1		0,5
	Возможно ли совмещение одним сотрудником должности администратора и сотрудника службы ИБ?		1		0	+	0,5
	Разработана ли политика безопасности организации?		0	+	1		0,5
	Устраивает ли сотрудников отношение руководства к ним?		0		1	+	0,5
	Увеличивается ли заработная плата сотрудников, при повышении квалификации?	+	0		1		0,5
	Разработана ли система премирования?	+	0		1		0,5
	Имеются ли письменные обязательства сотрудников о соблюдении конфиденциальности?		0	+	1		0,5
	Возможно ли использование сотрудниками неучтенных или нелицензионных программных продуктов?		1		0	+	0,5
	Имеется ли специальная система регистрации и контроля действий сотрудников, влияющих на ИБ?		0	+	1		0,5
Итого: 5,5/11=0,5							

Рис. 9. Лист опроса эксперта

Также модель теоретически может использовать в качестве нечетких лингвистических переменных вероятность преодоления средств защиты. Модель позволяет рассчитать вероятность реализации угрозы и при этом определяет риски реализации соответствующей угрозы.

Однако с помощью предложенной модели невозможно рассчитать время, затрачиваемое злоумышленником на реализацию угрозы, а также время обнаружения атаки.

Выводы

Проведенный анализ методов оценки рисков информационной безопасности показал, что метод на основе построения «Матрицы СУИБ» позволяет оценить степень защиты уже существующей СЗИ и степень выполнения всех требований по обеспечению информационной безопасности. Однако, данный метод не всегда применим к информационной системе, которая создается. Также для усовершенствования данного метода необходимо добавить несколько качественных шкал или возможность самостоятельно создавать шкалы по выбранному критерию оценивания.

Метод оценки рисков информационной безопасности на основе теории нечетких множеств даже при недостаточном объеме входных данных позволяет построить адекватную модель воздействия угроз на ресурс, который подлежит защите. При этом возможно рассматривать несколько ветвлений реализации угрозы или множества угроз на ресурс.

Таким образом, можно оценить наиболее вероятные угрозы на ИС и, на базе полученной информации, создать или модернизировать систему защиты информации.

Однако и этот метод имеет свои недостатки, поскольку не учитывает время реализации угрозы, а принимает во внимание только субъективную вероятность реализации угрозы или множества угроз.

Реализация угрозы может занять время большее, нежели информационный ресурс будет иметь ценность.

Поэтому для усовершенствования данного метода предлагается ввести коэффициент нормирования по времени согласно мнению эксперта при составлении опросных листов и проведении оценки рисков ИБ.

Список литературы

1. Домарев В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В.В. Домарев, Д.В. Домарев – Донецьк: Велстар, 2012. – 146 с.

2. Корниенко М.А. Модель оценки рисков информационной безопасности на основе теории нечетких множеств / М.А. Корниенко, Е.А. Островерхова // Материалы XVIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». Т. 4 – Х.: ХНУРЭ, 2014. – С. 279.

3. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко — К.: «МК-Пресс», 2006 - 320 с.

4. Матрица знаний информационной безопасности. Безопасность информационных технологий [Электронный ресурс]. – Режим доступа: http://domarev.com.ua.

5. Оценка СЗИ. Безопасность информационных технологий [Электронный ресурс]. – Режим доступа: http://domarev.com.ua.

6. Щербаков В.Б. Безопасность беспроводных сетей: стандарт IEEE 802.11 / В.Б. Щербаков, С.А. Ермаков. – М.: РадиоСофт, 2010. – 255 с.

Поступила в редколлегию 26.03.2014

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ МОДЕЛЕЙ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

О.А. Замула, О.В. Сєвєрінов, М.О. Корніенко

У даній статті розглянуті моделі оцінки ризиків інформаційної безпеки для аналізу інформаційних систем та побудови ефектних систем захисту інформації. Оцінка ризиків інформаційної безпеки проводиться відповідно з декількома моделями: на основі матриці системи управління інформаційною безпекою, включаючи якісні та кількісні шкали; на базі теорії нечітких множин.

Ключові слова: *оцінка ризиків інформаційної безпеки, система управління інформаційною безпекою, інформаційна безпека, нечітка логіка, нечіткі когнітивні карти.*

ANALYSIS OF INFORMATION SECURITY RISKS ASSESSMENT MODELS FOR BUILDING A DATA PROTECTION SYSTEM

A.A. Zamula, A.V. Severinov, M.A. Kornienko

This article describes the information security risks assessment models for analyzing information systems and building effective information security systems. Models were analyzed basing on the matrix of information security management system, including qualitative and quantitative scales and on the basis of the theory of fuzzy sets.

Keywords: *information security risks assessment, information security management system, information security, fuzzy logic, fuzzy cognitive maps.*