УДК 002.57

ОЦЕНКА РИСКА ВОЗДЕЙСТВИЯ НА ОБЪЕКТ ИНФОРМАТИЗАЦИИ С ПОМОЩЬЮ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ

В.Я. ИЩЕЙНОВ[1]
С.М. ЧУДИНОВ[2]

[1] Российский государственный гуманитарный университет,
[2] ОАО «СуперЭВМ», г. Москва

e-mail:
opr_dmitr@mail.ru
chud35@yandex.ru

В работе приведена оценка риска воздействия на объект информатизации с помощью аппарата нечетких множеств. Разработана, методика оценки эффективности защиты объекта информатизации. Предлагаемый метод позволяет произвести оценку риска, связанного с различными видами (типами) нарушителя и оценить конкретный риск для сопоставления его с допустимыми значениями.

Ключевые слова: информационная система, оценка риска, несанкционированное действие, модель нарушителя, рисковые показатели.

Методы защиты информации на объектах информатизации (и не только) классифицируются в соответствии с возможными каналами утечки: оптическим, акустическим, электромагнитным, материально-вещественным и т.п. и их (методов) может быть множество.

Можно выделить наиболее значимые из них:

– по целям действия (предупреждение, выявление, ...);

– по направлениям (правовая, организационная, инженерно-техническая ...);

– по виду угроз (целостность, конфиденциальность ...);

по объектам (территория, объект информатизации, автоматизированное рабочее место ...);

– по уровню охвата (групповая, индивидуальная ...);

– по активности (активная, пассивная).

Необходимо также рассматривать методы защиты информации по этапам работ.

1. Определение ресурсов, которые необходимо защищать.
2. Выявление угроз.
3. Оценка рисков.
4. Определение требований к системе защиты.
5. Выбор средств.
6. Внедрение.
7. Контроль за работой средств защиты.

В данной работе рассматриваются оценка риска воздействия на объект информатизации, имея в виду риск утраты конфиденциальной информации, т.е. безопасности для объекта информатизации.

В федеральном законе [1] записано, что безопасность – состояние защищенности жизненно важных интересов личности, общества и государства. Применительно к объекту информатизации понятие «безопасность» подразумевает его безопасность как критически важного объекта для защиты секретной, конфиденциальной информации, так как имеются риски потенциальных угроз воздействия на нее с целью хищения или воздействия.

Причиной возникновения таких угроз могут быть внешние воздействия, внутренние воздействия и стихийные бедствия.

Внешние и внутренние угрозы будем рассматривать с точки зрения возможного несанкционированного воздействия человека на объект информатизации.

Реализация потенциальных угроз безопасности объекта информатизации связана с неопределенностями, вызванными воздействиями различных факторов, которые могут порождать риски или способствовать их проявлению [2].

Риски воздействия на безопасность объекта информатизации могут быть реально опасными, в случае реализации конкретной угрозы в кризисной ситуации она оцениваются как вполне возможная, а величина порождаемого угрозой ущерба является значимой.

Рассмотрим оценку рисков при осуществлении несанкционированного доступа с помощью теории рисков [2], где оценки последствия риска представляются в виде вероятности посягательства нарушителя на объект информатизации, вероятности пресечения действий нарушителя и ущерба, который может быть от реализации угроз безопасности объекта информатизации.

Таким образом это запишется в виде:

$$Q=Ch(1-Сэф)U, \quad (1)$$

где Q – величина риска от несанкционированного доступа;

Ch – вероятность воздействия нарушителя на объект информатизации;

Сэф – вероятность эффективности защиты объекта информатизации;

(1-Сэф) – вероятность успешных действий нарушителя;

U – размер ущерба.

Расчет ожидаемого размера ущерба может быть рассчитан по формуле:

$$Uoy = \sum_j (1-\alpha ij \cdot Eij), \quad (2)$$

где αij – величина, характеризующая качественное влияние i – меры защиты, обеспечиваемой техническими средствами защиты (ТСЗ), при j – угрозе безопасности;

Eij – удельная эффективность ТСЗ.

Что должен сделать руководитель, решивший создать систему информационной безопасности? Наверное, выбрать приоритетные направления в этой области. Их может быть несколько. В общем случае это обеспечение доступности, конфиденциальности и целостности информации, иногда говорят еще о неотказуемости ее получения и создании системы физической защиты.

В зависимости от направления применяют различные средства защиты. Если наиболее значима конфиденциальность, т.е. угрозу для бизнеса представляет именно разглашение сведений, то наиболее эффективными при выстраивании защиты будут межсетевые экраны, средства разграничения доступа и антивирус.

Чем важнее информация, тем больше различных средств защиты придется установить, и тем сложнее могут быть их настройки.

Если первостепенным является гарантирование целостности информации, то полезно организовать резервное копирование и работать над увеличением надежности компьютерной системы – главное, уберечь информацию от случайных и намеренных искажений. Также актуальной в этом случае будет антивирусная защита.

Если предоставляется круглосуточный информационный ресурс, то очень важно, чтобы он был доступным. В этом случае свойство доступности окажется главным, для его обеспечения следует определенным образом организовать распределение нагрузки на серверах, осуществлять резервное копирование информации, применять антивирусную защиту.

Что касается конфиденциальности, то даже если это открытый информационный ресурс, работающий 24 часа в сутки, и все материалы на нем предоставляются бесплатно, пароли администратора необходимо держать в секрете. Это важно, так как если нарушитель получит доступ к Интернет-сайту, пользуясь привилегиями администратора, он сможет подменить документы, размещенные там, и пользователи получат недостоверную информацию. В этом случае свойства доступности и целостности информации будут нарушены, информация – искажена или удалена.

Все рассмотренные направления, кроме системы физической защиты, достаточно полно рассмотрены в различных источниках. На наш взгляд, важнее оценить вероятность успешных действий нарушителя, которые коррелируются с оценкой эффективности системы физической защиты.

Способы оценки каждой составляющей в формуле оценки риска (1) находятся в зависимости от имеющихся статистических данных и математических моделей исследуемого процесса.

Модель безопасности конфиденциальной информации в информационной среде разработана и рассмотрена в работе [3] в виде функциональной модели угроз безопасности:

$$Fy(t) = f\{F1(t), F2(t), F3(t), F4(t), F5(t), F6(t)\}, \quad (3)$$

где F1(t) – функция источника угроз;

F2(t) – функция угроз через каналы доступа;

F3(t) – функция угроз по способам реализации;

F4(t) – функция угроз через объекты воздействия;

F5(t) – функция угроз по виду информации;

F6(t) – функция угроз по виду нарушаемого свойства информации.

В связи с отсутствием статистических данных для оценки величин в формуле (1), и это в первую очередь связано с тем, что каждая система физической защиты объектов информатизации достаточно индивидуальная, предлагается применить для оценки теоретико-вероятностный метод, а именно метод нечетких множеств, оперирующий с интервальными (нечеткими) оценками.

Такой оценке подвергаются вероятность попыток нарушителя воздействовать на объект информатизации и последствия несанкционированных действий в случае их реализации.

Поскольку оценка последствий проводится на основании результатов, полученных с использованием теоретико-вероятностных методов, к сожалению, они не могут учесть весь спектр параметров (угроз), влияющих на процесс, в связи с чем оценка рисков будет иметь значительную погрешность.

Поэтому целесообразно использовать экспертные допущения, рассматривающие результаты уже проводимых оценок на другие конкретные случаи.

В основу метода нечетких множеств положена так называемая функция принадлежности μ(x), принимающая значения вероятности того, что x принадлежит некому множеству. С учетом того, что функция принадлежности будет строиться исходя из обработки мнений экспертов, они будут иметь дискретный (ступенчатый) характер, что определяется наличием конечного числа экспертов.

Для операций с функциями этого вида были разработаны специальные методы перемножения функций принадлежности, умножения на число и дефаззификация (получения точного значения) [4].

В предлагаемом методе используются следующие функции.

1. Функция Y(x) принадлежности привлекательности канала физической защиты (КФЗ) к вероятностному интервалу, область определения которой [0;1] и рассчитывается по формуле:

$$Y(x)=\frac{1}{H}\sum_{i=1}^{h} k_i \cdot vi(x), \qquad (4)$$

где H – число экспертов, участвующих в оценке;

h – число термов во множестве лингвистических переменных;

ki – число экспертов, использующих для описания i-ый терм;

vi(x) – функция принадлежности вероятности к i-ому терму.

Терм – лингвистическая переменная, принимающая значение из определенного множества (крайне привлекательно, очень привлекательно, привлекательно, мало привлекательно, непривлекательно).

2. Функция принадлежности вероятности к терму. Определяется экспертным методом путем графического сложения интервалов, которые каждый эксперт относит к терму.

3. Функция принадлежности частоты нападения на объект информатизации. Определяется экспертным путем. Обозначается C(x), область определения которой [0;∞].

4. Функция оценки последствий несанкционированного доступа (НСД). Обозначается U(x), определяется экспертным путем на объекте информатизации и представляет собой функцию принадлежности последствий доступа определенному интервалу последствий НСД.

5. Степень принадлежности последствий НСД к тому или иному интервалу. Интервал последствий НСД – диапазон последствий НСД, определяемый нормативными документами, – относящихся к одной категории (локальных, местных, территориальных, региональных последствий НСД).

Применение аппарата нечетких множеств разбивается на несколько этапов.

Вначале определяется модель нарушителя. Далее проводится опрос экспертов и определяются зависимости привлекательности КФЗ для конкретной модели нарушителя в зависимости от эффективности системы физической защиты (СФЗ) и последствий НСД.

На следующем этапе проводится опрос экспертов о связи термов с числовыми значениями, на основе которых строится функция принадлежности вероятности к терму. После чего на основании выбора термов, полученных ранее, и функции принадлежности вероятности к терму по формуле (4) рассчитываем привлекательность КФЗ (Y(x)) с учетом эффективности его СФЗ и последствий НСД.

Затем определяется функция принадлежности частоты нападений на объект информатизации конкретным типом нарушителя (C(x)). Опрашиваемые эксперты должны дать прогноз того, как часто (раз в определенный момент времени) нарушитель рассматриваемого типа может посягнуть на объект информатизации.

В соотношении (1) вероятность посягательств нарушителя оценивается как произведение частоты посягательства на объект информатизации и показателя привлекательности КФЗ:

$$Ch = Y(x) \cdot C(x). \quad (5)$$

На следующем этапе силами объектовых и других привлеченных экспертов строится функция оценки возможных последствий НСД для данного КФЗ. Масштаб последствий НСД при наличии соответствующей методики мог бы быть оценен достаточно точно, однако, в большинстве случаев существует неопределенность в исходных данных, что снижает точность оценки. Поэтому для определения последствий НСД наиболее применим экспертный метод, но эксперты должны быть ознакомлены с расчетными оценками последствий НСД в наихудших случаях.

Соответственно эксперты могут дать оценку только в виде интервалов. Чем уже интервал, тем точнее оценка, тем больший вес должно иметь мнение эксперта. Поэтому при сложении «высота» интервала должна быть обратно пропорциональна его длине.

Для расчета вводится значение li – длины интервала, которая равна разнице между наибольшим значением интервала и его наименьшим значением. Максимальный интервал обозначим как lmax. Тогда «высота» интервала определяется из соотношения:

$$Yi = (lmax / li) \cdot k, \quad (6)$$

где k – определяется из условия $\sum_{i=1}^{h} Y_i = 1.$

Далее проводится оценка эффективности защиты объекта информатизации. В случае если область определения функции принадлежности последствий НСД охватывает два и более интервала, тогда необходимо определить интегральную функцию привлекательности. Для этого функции привлекательности, соответствующие каждому из интервалов, должны быть умножены на коэффициент принадлежности последствий к интервалу (проведено нормирование) и полученные функции принадлежности сложены между собой.

Затем необходимо провести умножение функции принадлежности частоты на привлекательность и на (1-Сэф), в результате получается функция принадлежности индивидуального риска в зоне поражения. Умножение на функцию принадлежности, описывающую ущерб (или на точное значение ущерба, если имеется возможность его оценки), позволяет получить значение материального риска.

С учетом ступенчатого вида функций принадлежности, а также имеющейся специфики работы с функциями принадлежности, необходимо описать алгоритмы их умножения [4].

Операция умножения нечетких чисел (интервалов) обозначается через

$$Y \cdot \nu = U\{\delta, \mu(\delta)\}, \quad (7)$$

где функция принадлежности результата $\mu(\delta)$ определяется по формуле [4]:

$$\mu(\delta) = \sup\{\min\{\mu(x), \mu(y)\}\}, \quad (8)$$

где $\delta = x \cdot y$.

Указанная операция для рассматриваемого типа функций принадлежности достаточно легко выполняется расчетом на ЭВМ.

Для того чтобы от функции принадлежности перейти к точному значению риска, используются методы дефаззификации, например, с помощью определения «центра тяжести» или «центра площади» [4].

Таким образом, для каждой модели нарушителя и для каждого КФЗ определяются показатели риска в виде частоты возникновения рискового события или стоимостной оценки ущерба в зависимости от решаемой задачи.

Поле распределения показателей представляется в виде таблицы.

Таблица

Поле распределения рисковых показателей

	КФЗ1	КФЗ2	...	КФЗi	
Модель 1					i-й по строке риск – риск при действиях данного типа нарушителя
Модель 2					
...					
Модель i					
	i-й по столбцу риск для конкретного КФЗ				

Из рассмотрения поля распределения рисковых показателей следует, что максимальное значение риска в строке есть максимальный риск при действиях конкретного типа нарушителя.

Предлагаемый метод с применением аппарата нечетких множеств позволяет произвести оценку риска, связанного с различными видами (типами) нарушителя и оценить конкретный риск для сопоставления его с допустимыми значениями.

Список литературы

1. Федеральный закон от 28.12.2010 г. №390-ФЗ «О безопасности».
2. Вишняков Л.Д., Радаев Н.И. Общая теория рисков. – М.: Академия, 2007.
3. Ищейнов В.Я., Чудинов С.М. Модель безопасности конфиденциальной информации в информационной системе // Научные ведомости Белгородского государственного университета, 2012. – Вып. 23/1, №13 (132).
4. Леоненков А.В. Нечетное моделирование в среде Matlab fuzzy TECH. – СПб.: БХВ-Петербург, 2005.

RISK ASSESSMENT OF IMPACT ON PROPERTY INFORMATION BY FUZZY SETS

V.J.ISCHEYNOV[1]
S.M. CHUDINOV[2]

[1]) RGGU ,
[2]) NII «SuperEVM», Moscow

e-mail:
opr_dmitr@mail.ru chud35@yandex.ru

This paper provides estimates of risk from exposure to the object information using fuzzy sets. Developed method of estimating the efficiency of information asset protection. The proposed method allows to assess the risk associated with different types (types) of the offender and assess the specific risk to match it with the correct values.

Keywords: information system, risk assessment, the unauthorized action, of the model offender, risk indicators.