УДК 004.056

ПОСТРОЕНИЕ ЭКСПЕРТНОЙ СИСТЕМЫ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ БАЙЕСОВСКОГО ПОДХОДА

И.А. Будовских, Ю.Н. Загинайлов
Алтайский государственный технический университет им. И.И. Ползунова
г. Барнаул

Статья посвящена разработке алгоритма работы экспертной системы для оценки угроз безопасности персональных данных в информационной системе на основе байесовского подхода.

Ключевые слова: экспертная система, оценка угроз безопасности, персональные данные, информационная система.

Оценка угроз безопасности персональных данных (ПДн) в информационной системе их обработка является неотъемлемой частью разработки модели угроз, на основе которой анализируется исходное состояние защищенности и строится система защиты информации для неё [1]. В связи с этим, процесс оценки угроз занимает важное место при обеспечении защиты информации в информационных системах персональных данных (ИСПДн).

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является одним из регуляторов в области защиты информации и на 2016 год имеет два методических документа, которые затрагивают область оценки угроз информационной безопасности:

1) «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена 14 февраля 2008 года [2].

2) «Методика определения угроз безопасности информации в информационных системах» [3]. Данный документ является проектом и после его утверждения он сменит методику [2]. Применимость этого документа для государственных информационных систем рассмотрена в [4].

В методике [2] «под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя». В методике [3], осуществление оценки угроз информационной безопасности предполагается экспертной группой, рекомендации по формированию которой, подробно изложены в этом же документе.

Независимо от результата формирования группы при оценке угроз информационной безопасности существуют субъективные факторы, связанные с психологией принятия решения человеком. Это может приводить к занижению или завышению оценки, что в свою очередь, приводит к пропуску отдельных угроз или к неоправданным затратам на нейтрализацию не актуальных угроз.

Другой проблемой защиты информации, вытекающей из субъективной экспертной оценки угроз, является сложность проведения аудита информационной безопасности ИСПДн, так как при аудите, особенно внешнем, эксперты могут не подтвердить актуальные угрозы, определённые экспертами при проектировании (создании) системы защиты ИСПДн или выполнившими внутренний аудит, не подтвердить типы угроз, или в соответствии с угрозами, определить необходимость применения криптографических средств защиты информации, а это в свою очередь может привести к затруднению (приостановлению) какого либо вида деятельности оператором этой ИСПДн.

В качестве варианта решения данного рода проблем, была построена экспертная система (ЭС, понятие ЭС подробно рассмотрено в [5]) оценки угроз информационной безопасности на основе байесовского подхода.

Исходными данными для ЭС оценки угроз информационной безопасности (ЭСОУБ) являются:

1) Множество угроз информационной

безопасности УИБ[N].

2) Частота (априорная вероятность) встречаемости угроз P_0(УБИ$_i$). Оценка экспериментальная. Например, если из 1000 опрошенных организаций 30 подверглись реализации угрозы, то частота равна 0,03. Так же информация может быть взята из литературы и других материалов. Сумма УБИ$_i$ может не равняться 1.

3) Перечень условий реализации угроз УР[N] (вопросы, задаваемые ЭС). Например, «Оборудовано ли помещение, в котором обрабатываются персональные данные охранной сигнализацией?». Одной УБИ$_i$ может быть поставлено в соответствие множество УР$_j$.

4) Условная вероятность Ру=P(УР$_j$/УБИ$_i$). Вероятность УР$_j$ угрозы, если УБИ$_i$ действительно существует. Оценка Ру экспериментальная, осуществляется по аналогии с P_0.

5) Условная вероятность Pn=P(УР$_j$/notУБИ$_i$). Вероятность УР$_j$ угрозы, если УБИ$_i$ отсутствует. Оценка Pn экспериментальная, осуществляется по аналогии с P_0.

6) Обратная условная вероятность Qy=1-Py=P(notУР$_j$/УБИ$_i$). Вероятность реализации УБИ$_i$ при отсутствии условия реализации УР$_j$.

7) Обратная условная вероятность Qn=1-Pn=P(notУР$_j$/notУБИ$_i$). Вероятность реализации УБИ$_i$ при отсутствии УР$_j$ и самой УБИ$_i$.

Все исходные данные, в совокупности формируют базу знаний, от достоверности которой зависит достоверность результатов работы ЭСОУБ.

На рисунке 1 представлена схема взаимосвязи входных параметров ЭКОУБ.

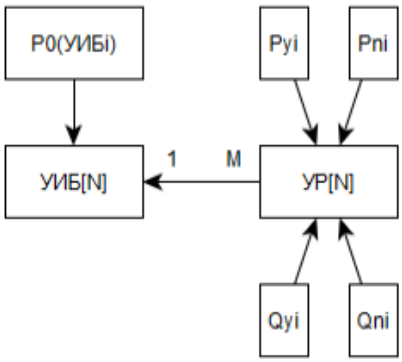

Рисунок 1 – Схема взаимосвязи входных параметров ЭСОУБ

На рисунке 2 представлена обобщенная блок-схема работы ЭСОУБ.

Рассмотрим блок-схему ЭСОУБ подробнее.

На первом этапе осуществляется считывание данных из базы знаний.

На втором этапе осуществляется запуск цикла с предусловием wihle, который будет выполнять этапы 3-6 до тех пор, пока в блоке 6 не будет выставлен флаг завершения.

Третий этап работы ЭСОУБ включает в себя выбор наиболее значимого вопроса УР$_j$ из перечня УР[N] не исключенных и вывести его на экран пользователю. Значимость УР$_j$ определяется в зависимости от того, к скольким УБИ$_i$ он относится. Чем больше число отношений, тем выше значимость. Если вопросов с одним и тем же количеством отношений несколько, то выбор осуществляется с помощью датчика случайных чисел.

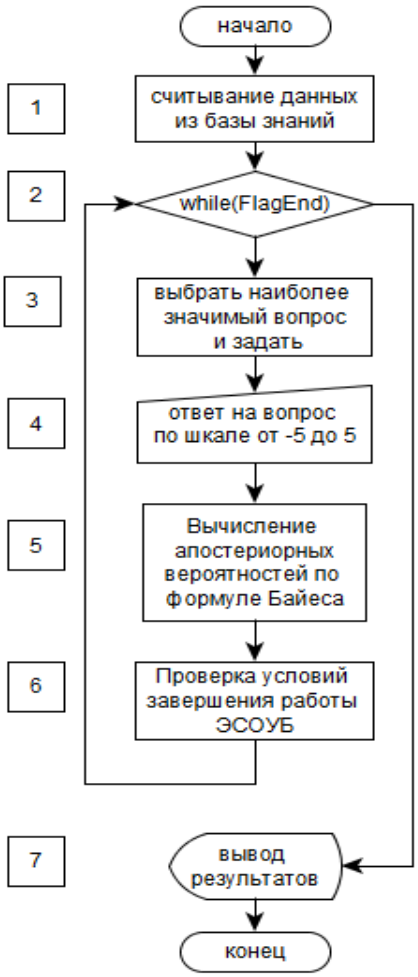

Рисунок 2 – Обобщенная блок-схема функционирования ЭСОУБ

Затем происходит исключение текущего $УР_j$ из перечня УР[N] для того, чтобы избежать повторения на следующей итерации цикла.

На четвертом этапе осуществляется считывание данных введенных с клавиатуры пользователем. Данные варьируются по шкале от -5 до 5 с шагом 1. Значение «-5» - абсолютно нет, значение «5» - абсолютно да.

На пятом этапе осуществляется вычисление апостериорных вероятностей в зависимости от ответа:

1) Для ответа «5» на вопрос $УР_j$, для $УБИ_i$ вычисляется апостериорная вероятность P_+ по формуле (1):

$$P_+=Py*Pc/(Py*Pc+Pn*Qc), \quad (1)$$

где Pc – текущая вероятность реализации угрозы, Qc – обратная вероятность (1-Pc).

Далее значение Pc приравнивается вычисленному значение P_+.

2) Для ответа «-5» на вопрос $УР_j$, для $УБИ_i$ вычисляется апостериорная вероятность P_- по формуле (2):

$$P_-=Qy*Pc/(Qy*Pc+Qn*Qc). \quad (2)$$

Далее значение Pc приравнивается вычисленному значение P_-.

3) Если ответ «0» значение Pc не меняется.

4) Для ответов «1, 2, 3, 4» значение апостериорной вероятности Pk определяется уравнением (3):

$$(Pk – P_0)/(P_+-P_0)=k/5, \quad (3)$$

где k = {1,2,3,4}.

Выразив значение Pk из (3) получим формулу для ее вычисления (4):

$$Pk=k*(P_+ - P_0)/5 - P_0. \quad (4)$$

5) Для ответов «-1, -2, -3, -4» значение апостериорной вероятности Pk определяется уравнением (5):

$$(Pk – P_0)/(P_0-P_-)=k/5, \quad (5)$$

где k = {-1,-2,-3,-4}.

Выразив значение Pk из (5) получим формулу для ее вычисления (6):

$$Pk=k*(P_0 – P_-)/5 + P_0. \quad (6)$$

На шестом этапе работы существляется проверка условия завершения ЭСОУБ. Условие считается выполненым, если все вопросы $УР_j$ исключены из перечня УР[N].

На данном этапе ЭСОУБ завершает работу и упраление передается в блок вывода результатов.

Сложность реализации такой системы заключается в сборе информации для базы знаний, а также поддержке ее в актуальном состоянии. Это обусловлено тем, что в настоящее время информационные технологии бурно развиваются, следовательно, растет перечень угроз информационной безопасности. Для этих целей может быть использована база угроз безопасности информации размещённая на официальном сайте ФСТЭК России, которая постоянно актуализируется.

По сравнению с методиками [2] и [3], где оценка осуществляется посредством вербальной интерпретации (актуальна, неактуальна), подобная система позволит точно определить вероятность реализации угроз, что, в свою очередь, позволит выгодней распределить бюджет организации и избежать не оправданных затрат. Так же она позволит осуществлять оценку угроз безопасности ИСПДн без влияния субъективного фактора и появления возможных «разногласий» по мерам защиты между оператором ИСПДн и внешним аудитором.

Следующим этапом работы в данном направлении будет сбор информации для базы знаний, определения методики использования базы УБИ ФСТЭК России, автоматизация и исследование системы.

СПИСОК ЛИТЕРАТУРЫ

1. Базовая модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных: утв. Федеральной службой по техническому и экспортному контролю 15.02.08: ввод в действие с 15.02.08.
2. Методика определения актуальных угроз безопасности персональных данных при их обработки в информационных системах персональных данных: утв. Федеральной службой по техническому и экспортному контролю 14.02.08: ввод в действие с 14.02.08.
3. Методика определения угроз безопансоти в информационных системах: проект. Федеральная служба по техническому и экспортному контролю.
4. Будовских И.А., Загинайлов Ю.Н., Оценка применимости для аудита безопасности государственных ИС методики определения угроз безопасности информации, разработанной ФСТЭК России**.** Измерение, контроль, информатизация: материалы XVII международной научно-технической конференции. /под ред. Л.И. Сучковой. – Барнаул: Изд-во АлтГТУ, 2016. – 287 с.240-243.
5. Нейлор К. Как построить свою экспертную систему: Пер. с анг. – М.: Энергоатомиздат, 1991. -286 с.: ил. ISBN 5-283-02502-0.

Загинайлов Юрий Николаевич – к.в.н., доцент, тел.: (3852) 290-718, e-mail: zun25@mail.ru;
Будовских Иван Андреевич – магистрант, e-mail: ivan.budovskih@yandex.ru.