УДК 004.056.5

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ДЛЯ АНАЛИЗА И ОЦЕНКИ УРОВНЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Олег Александрович Зеленский**, студент*
Тел.: 8-915-005-33-71, e-mail: zel-oleg@mail.ru,
Московский авиационный институт (национального исследовательского университета)
http://www.mai.ru
***Александр Григорьевич Зеленский**, к. физ.-мат. н., доц.*
Тел. 8-916-376-44-59, e-mail: zel-alex@mail.ru
Московский университет им. С.Ю. Витте
http://www.miemp.ru

Излагается построение расширенной математической модели для анализа и оценки уровня угроз безопасности персональных данных в информационных системах с применением формализованных экспертных знаний.

Ключевые слова: информационная система, персональные данные, математическая модель, уровень угроз безопасности, экспертные оценки

На сегодняшний день защита персональных данных (ПДн) является актуальной задачей, поскольку в большинстве крупных организаций существуют информационные системы, в которых хранятся персональные данные.


О. А. Зеленский

Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 25.07.2011) [1, с. 1] персональные данные – это любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту) персональных данных.

Проблема защиты персональных данных существует давно и является далеко не простой технической или экономическая проблемой. Она включает в себя, в том числе, неадекватное и нецелесообразное собирание сведений о своих клиентах или работниках, а также дальнейшее небрежное их использование и хранение.


А. Г. Зеленский

Одна из наиболее важных задач в области защиты ПДн это разработка модели угроз безопасности.

Для того чтобы разработать модель угроз безопасности конкретной информационной системы (ИС), необходимо составить перечень всевозможных угроз безопасности для ПДн, которым может быть подвержена исследуемая ИС, с учетом анализа информационных процессов организации и особенностей реализации ИС.

Следующим шагом на пути решения поставленной задачи является выбор наиболее актуальных угроз из общего списка. Для этого необходимо ввести следующие понятия и определения.

Систему защиты ПДн в ИС можно описать с помощью кортежа

<O,A,B> [2, с. 14–15],

где:O = {Oh} –множество объектов защиты персональных данных, образующих информационную систему;
A = {ai} –множество угроз для информационной системы;
B = {bi} – множество средств противодействия угрозам.

Согласно [3, с. 6] актуальной считается угроза ai, которая может быть реализована в информационной системе и представляет опасность для ПДн.

Для оценки возможности реализации угрозы применяются два показателя [3, с. 6]: уровень исходной защищенности ИС γ и частота (вероятность) реализации рассматриваемой угрозы p_i. Под уровнем исходной защищенности ИС понимается обобщенный показатель, зависящий от уровня защищенности технических и эксплуатационных характеристик ИС u_i, приведенных в табл. 1.

Таблица 1

Показатели исходной защищенности ИС

Технические и эксплуатационные характеристики ИС	Уровень защищенности u_i		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
– распределенная ИС, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
– городская ИС, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
– корпоративная распределенная ИС, охватывающая многие подразделения одной организации;	–	+	–
– локальная (кампусная) ИС, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
– локальная ИС, развернутая в пределах одного здания.	+	–	–
2. По наличию соединения с сетями общего пользования:			
– ИС, имеющая многоточечный выход в сеть общего пользования;	–	–	+
– ИС, имеющая одноточечный выход в сеть общего пользования;	–	+	–
– ИС, физически отделенная от сети общего пользования.	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
– чтение, поиск;	+	–	–
– запись, удаление, сортировка;	–	+	–
– модификация, передача.	–	–	+
4. По разграничению доступа к персональным данным:			
– ИС, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИС, либо субъект ПДн;	–	+	–
– ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС;	–	–	+
– ИС с открытым доступом.	–	–	+
5. По наличию соединений с другими базами ПДн иных ИС:			
– интегрированная ИС (организация использует несколько баз ПДн ИС, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
– ИС, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИС.	+	-	-
6. По уровню обобщения (обезличивания) ПДн:			
– ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
– ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
– ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки:			
– ИС, предоставляющая всю базу данных с ПДн;	–	–	+
– ИС, предоставляющая часть ПДн;	–	+	–
– ИС, не предоставляющая никакой информации.	+	–	–

Исходная степень защищенности ИС γ определяется следующим образом [3, с. 7]:

1. ИС имеет высокий уровень исходной защищенности (γ = «высокий»), если не менее 70% характеристик ИС соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные среднему уровню защищенности (положительные решения по второму столбцу);

2. ИС имеет средний уровень исходной защищенности (γ = «средний»), если не выполняются условия по пункту 1 и не менее 70% характеристик ИС соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные низкому уровню защищенности;

3. ИС имеет низкую степень исходной защищенности (γ = «низкий»), если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент [3, с. 8], а именно:

$Y_1 = 0$ – для высокой степени исходной защищенности (γ = "низкий");

$Y_1 = 5$ – для средней степени исходной защищенности (γ = "средний");

$Y_1 = 10$ – для низкой степени исходной защищенности (γ = "высокий").

Под частотой (вероятностью) реализации угрозы p_i понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИС в складывающихся условиях обстановки.

Вводятся четыре вербальных градации этого показателя [3, с. 8]:

p_i = "маловероятно" – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

p_i = "низкая " – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

p_i = "средняя " – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

p_i = "высокая " – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2^i [3, с. 8], а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

Y^iС учетом вышеизложенного, коэффициент реализуемости угрозы будет определяться соотношением

$$Y^i = (Y_2^i + Y_1)/20.$$

По значению коэффициента реализуемости угрозы Y^i формируется вербальная интерпретация реализуемости угрозы $Z_i = Z(Y^i)$ следующим образом:

если $0 \le Y^i \le 0.3$, то возможность реализации угрозы признается низкой (Z^i= «низкая»);

если $0.3 < Y^i \le 0.6$, то возможность реализации угрозы признается средней (Z^i = «средняя»);

если $0.6 < Y^i \le 0.8$, то возможность реализации угрозы признается высокой (Z^i = «высокая»);

если больше 0.8, то возможность реализации угрозы признается очень высокой (Z^i = «очень высокая»).

Далее оценивается опасность каждой угрозы X^i. При оценке опасности на основе опроса специалистов в области защиты персональных данных определяется вербальный показатель опасности для рассматриваемой ИС. Этот показатель может иметь следующие значения:

X^i = "низкая" – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

X^i = "средняя" – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

X^i = "высокая" – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего перечня угроз безопасности тех, которые относятся к актуальным, с помощью табл. 2 [3, с. 8].

Таблица 2

Правила отнесения угрозы a_i к актуальной

Возможность реализации угрозы Z^i	**Показатель опасности угрозы X^i**		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Вышеизложенную математическую модель анализа и оценки уровня угроз безопасности персональных данных в информационных системах можно представить в виде блок-схемы, изображенной на рисунке 1.

Представленную математическую модель анализа и оценки уровня угроз безопасности персональных данных необходимо использовать уже на этапах проектирования и внедрения ИС в организации с целью уменьшения расходов и повышения уровня безопасности при последующем ее функционировании.

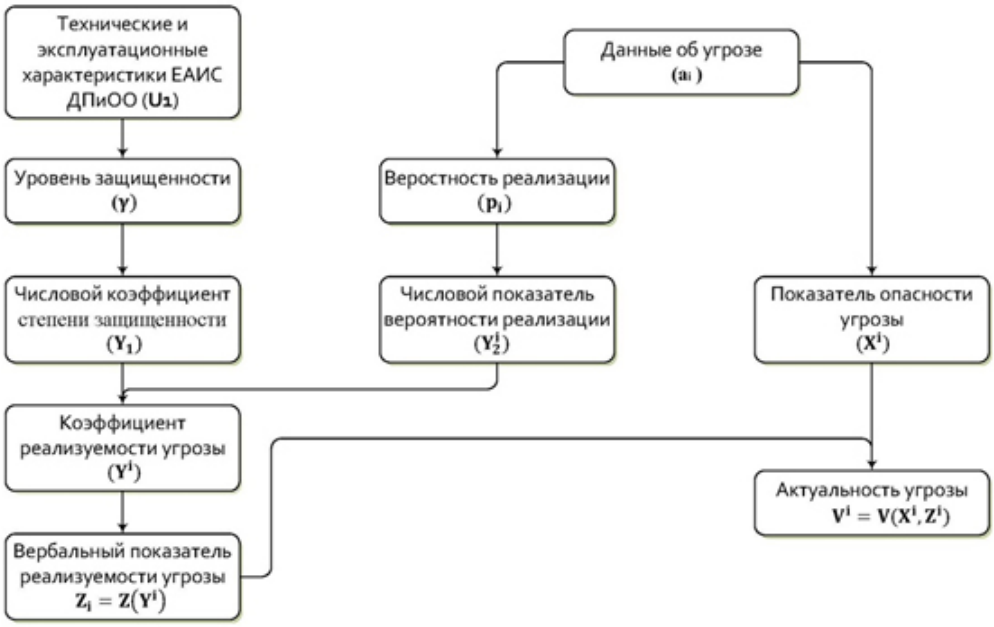

Рис. 1. Блок-схема математической модели анализа и оценки уровня угроз безопасности персональных данных в информационных системах

Заключение. Предлагаемая расширенная математическая модель для анализа и оценки уровня угроз безопасности персональных данных в ИС основана на базовой системной модели ИС и применении формализованных экспертных знаний. Применение данной модели необходимо использовать уже на этапах проектирования и внедрения ИС в организации с целью уменьшения расходов и повышения уровня безопасности при последующем ее функционировании.

Литература

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (ред. от 25.07.2011).

2. *Васильев В.И., Бакиров А.А., Бабиков А.Ю*. Математическая модель для анализа защищенности взаимосвязанных информационных объектов // Проблемы информационной безопасности. Компьютерные системы. 2000. №1. С. 13–19.

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 г.

Creation of mathematical model for analysis and assessment of level of threats to personal information security in information systems

Oleg Aleksandrovich Zelensky, student
Moscow aviation institute (national research university)

Alexander Grigoryevich Zelensky, candidate of physical and mathematical sciences, associate professor
Moscow University after S.V.Vitte

The creation of expanded mathematical model for the analysis and an assessment of the level of threats to the personal information security in information systems with application of the formalized expert knowledge is presented.

Keywords: information system, personal information, mathematical model, level of threats to security, expert estimates.