3. *Хомский Н.* Десять способов манипулирования с помощью средств массовой информации (Diez formas distintas de manipulación mediática). Rebellion. Испания, 2011.

4. *Мурсалиева Г.* Группы смерти // Новая газета. № 51. 16.05.2016.

УДК 004.512.2

М. А. Пермякова
Научный руководитель: О. В. Пермякова
Магнитогорский государственный технический университет,
Магнитогорск

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДИКИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ ИБ В ИСПДн

Аннотация. При исследовании ИСПДн составляется модель угроз, в которой даны описание класса ИСПДн и возможные источники угрозы безопасности персональных данных. В ходе составления данной модели рассчитываются коэффициенты реализуемости угроз и проверяется актуальность УБПДн. Расчет необходимых параметров производится в приложении, созданном на языке C#.

Ключевые слова: угроза безопасности персональных данных; информационная система персональных данных; коэффициент реализуемости угрозы; актуальность угрозы.

Угрозы безопасности персональных данных (УБПДн) представляют собой совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн [1].

УБПДн реализуются в результате образования канала реализации угроз между источником угрозы и источником ПДн. Основные элементы канала реализации УБПДн представлены на рис. 1.

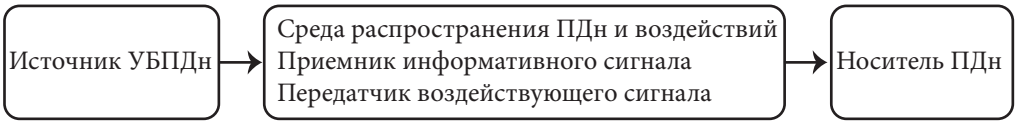

Рис. 1. Обобщенная схема канала реализации УБПДн

В соответствии с видами источников УБПДн делятся на:

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая внутренних нарушителей;
– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования (внешние нарушители).

Нарушители, согласно Банку данных угроз ФСТЭК, могут иметь разный потенциал: низкий, средний, высокий, а также различные комбинации внешних и внутренних нарушителей. Возможности внутреннего нарушителя зависят от режимных и организационно-технических мер защиты, сами нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

Согласно ФЗ «О персональных данных» № 152-ФЗ от 27 июля 2006 г. ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий [2]. Безопасность персональных данных при их обработке в ИС обеспечивается с помощью системы защиты ПДн, нейтрализующей актуальные угрозы, т. е. угрозы, которые могут быть реализованы в ИСПДн и представляют опасность для ПДн. Система защиты ПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных УБПДн и информационных технологий, используемых в ИС. Для оценки возможности реализации угрозы применяются уровень исходной защищенности ИСПДн и вероятность реализации данной угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Данные характеристики сформированы в таблице, которая приведена в методике определения актуальных угроз [3]. После чего уровню исходной защищенности в соответствие ставится числовой коэффициент $Y1$, в зависимости от степени исходной защищенности.

Вероятность реализации угрозы — это определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной УБПДн для данной ИСПДн. Существует четыре градации этого показателя:

– маловероятно;
– низкая вероятность;
– средняя вероятность;
– высокая вероятность.

Для каждой градации в соответствие ставится числовой коэффициент *Y*2. Таким образом, коэффициент реализуемости угрозы будет определяться по формуле:

$$Y = \frac{Y_1 + Y_2}{20}.$$

По значению коэффициента реализуемости угрозы *Y* формируется интерпретация реализуемости угрозы: низкая, средняя, высокая и очень высокая. Затем необходимо оценить опасность каждой угрозы, у которой есть три показателя: низкая, средняя и высокая. После чего осуществляется выбор из предварительного перечня угроз тех, которые относятся к актуальным для данной ИСПДн, в соответствии с табл. 1.

Таблица 1

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
низкая	неактуальная	неактуальная	актуальная
средняя	неактуальная	актуальная	актуальная
высокая	актуальная	актуальная	актуальная
очень высокая	актуальная	актуальная	актуальная

Для оптимизации расчета коэффициентов было разработано приложение с использованием языка программирования C# (рис. 2). Пользовательский интерфейс предполагает выбор необходимых параметров для выполнения рас-

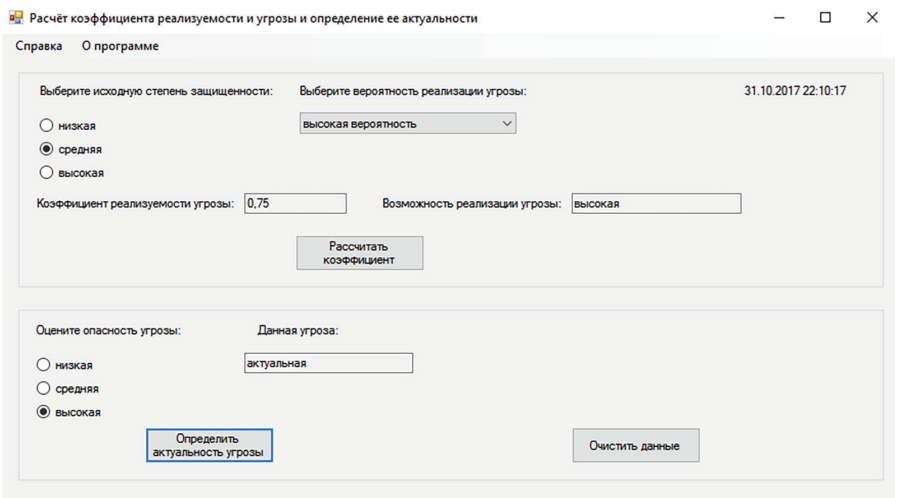

Рис. 2. Общий вид главного диалогового окна приложения

четов. После получения коэффициента реализуемости угрозы нужно оценить опасность данной угрозы и определить ее актуальность. В контекстном меню программы дано описание документов, на которых основаны все расчеты.

Конкретные организационно-технические требования по защите ИСПДн от НСД, выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн, формулируются на основе составленного перечня актуальных угроз.

Список литературы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) (утв. ФСТЭК РФ 15.02.2008).

2. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008).

УДК 378.147

С. А. Сабельников
Научный руководитель: д-р пед. наук, проф. Л. В. Астахова
Южно-Уральский государственный университет, Челябинск

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМЫ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ КОРПОРАТИВНЫХ СИСТЕМ К AGILE-УПРАВЛЕНИЮ ПРОЕКТАМИ

Аннотация. В статье описаны методические подходы, лежащие в основе педагогической системы подготовки будущих специалистов по защите корпоративных систем к agile-управлению проектами.

Ключевые слова: подготовка будущих специалистов по защите корпоративных систем в вузе; метод проектов в образовании; защита информации; управление проектами; методологии agile.

Исследование проблемы подготовки будущих специалистов по защите корпоративных систем к agile-управлению проектами позволило определить, что