УДК004.42

ПРОГРАММНЫЙ МОДУЛЬ ПОСТРОЕНИЯ МОДЕЛИ НАРУШИТЕЛЯ ДЛЯ ИСПДН

А.В. ВЛАСЕНКО, К.В. КЛИМЕНКО, Ю.Е. ЕГОРИХИН, Е.И. КАШИРИНА

Кубанский государственный технологический университет
350072, Российская Федерация, г.Краснодар, ул.Московская, 2
электронная почта:Vlasenko@kubstu.ru, elivkashir@yandex.ru

Разработка программного модуля построения модели нарушителя для ИСПДн, написанного на языке C#, позволяющего автоматизировать процесс создания модели нарушителя по документам ФСТЭК и ФСБ.
Ключевые слова: модель угроз, модель нарушителя, ИСПДн, программный модуль.

Применение информационных технологий (ИТ) требует повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести компании значительный материальный ущерб. Без должной степени защиты информации внедрение ИТ может оказаться экономически невыгодным в результате значительных потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях. Поэтому, в настоящее время актуальным является разработка программного модуля построения модели нарушителя для информационной системы персональных данных (ИСПДн).

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

– целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;

– конфиденциальность информации;

– доступность информации для всех авторизованных пользователей.

Целью определения угроз безопасности информации является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации,

содержащейся в информационной системе, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных. Определение угроз безопасности информации должно носить систематический характер и осуществляться как на этапе создания информационной системы и формирования требований по ее защите, так и в ходе эксплуатации информационной системы.

В обобщенном виде угрозы безопасности информации характеризуется источниками угроз, факторами, обуславливающими возможность реализации угроз, способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации. Важным этапом в процессе определения угроз безопасности информации является идентификация лиц или событий (явлений), в результате действий (наступления, возникновения) которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и возникновение неприемлемых негативных последствий (ущерба).

Для автоматизации процесса построения модели нарушителя для ИСПДн был разработан программный модуль, написанный на языке C#, позволяющий построить модель нарушителя, опираясь как на документыФедеральной службы по техническому и экспертному контролю (ФСТЭК), так и на документацию Федеральной службы безопасности(ФСБ).

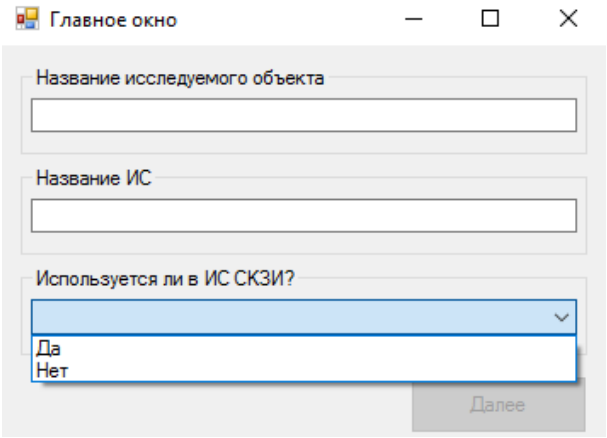

Рисунок 1 – Главное окно программного модуля

Если же в информационной системе имеются средства криптографической защиты информации (СКЗИ), то модель нарушителя будет базироваться на документах ФСБ.

На рисунке 2 обозначены категории нарушителей, из которых требуется выделить представляющие для конкретно взятой ИСПДн угрозу, основываясь на имеющихся сведениях о данной информационной системе.

При ответе положительно на любой из вопросов 1-10 – информационной системе (ИС) присваивается класс защищенности КС1. При положительном ответе хотя бы на один вопрос 11-14 – системе присваивается класс защищенности КС2. Если имеется положительный ответ на вопрос 15-16 – ИС присваивается класс защищенности КС3.При положительном ответе на любой вопрос 18-19 – информационной системе присваивается класс защищенности КВ. При данном положительном ответе на вопрос 20-22 – выбранной системе присваивается класс защищенности КА[1].

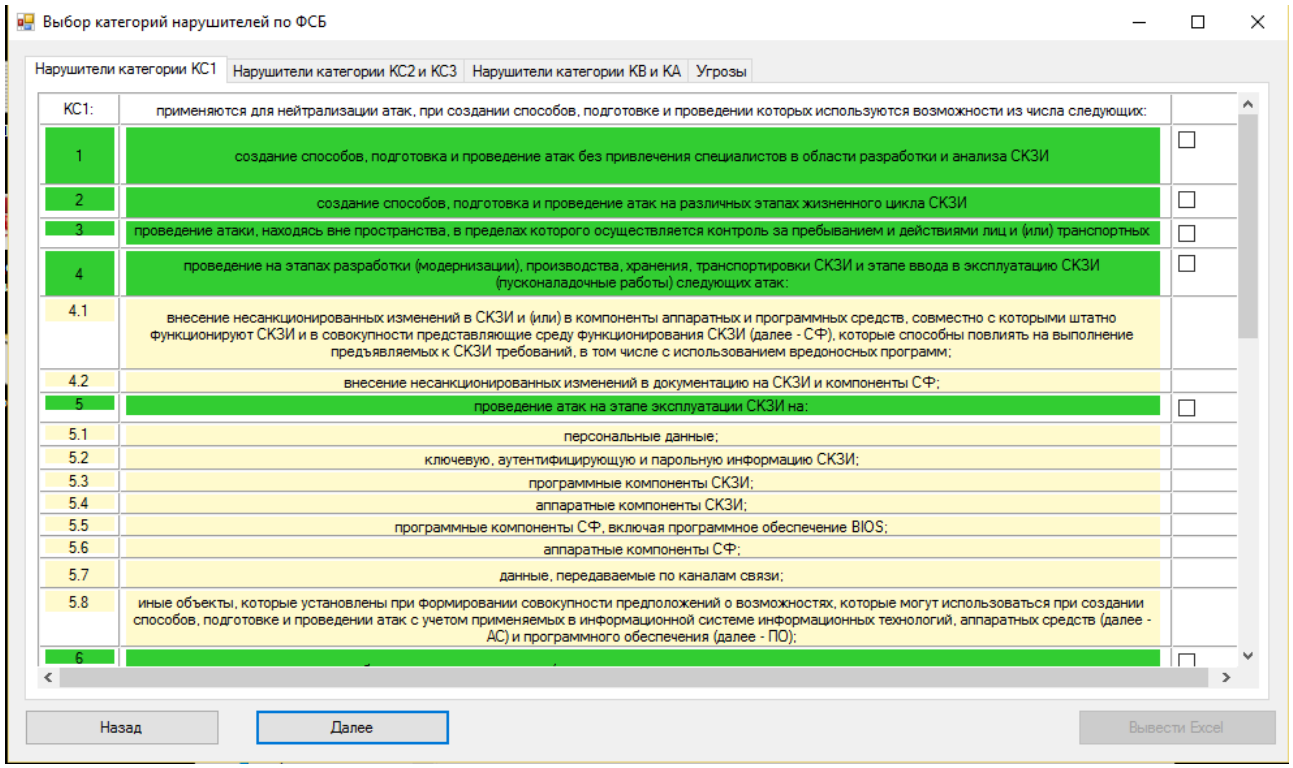

Рисунок 2 – Выбор категорий нарушителя по ФСБ

Следующим шагом будет определение актуальных угроз безопасности для взятой системы. (рисунок 3).

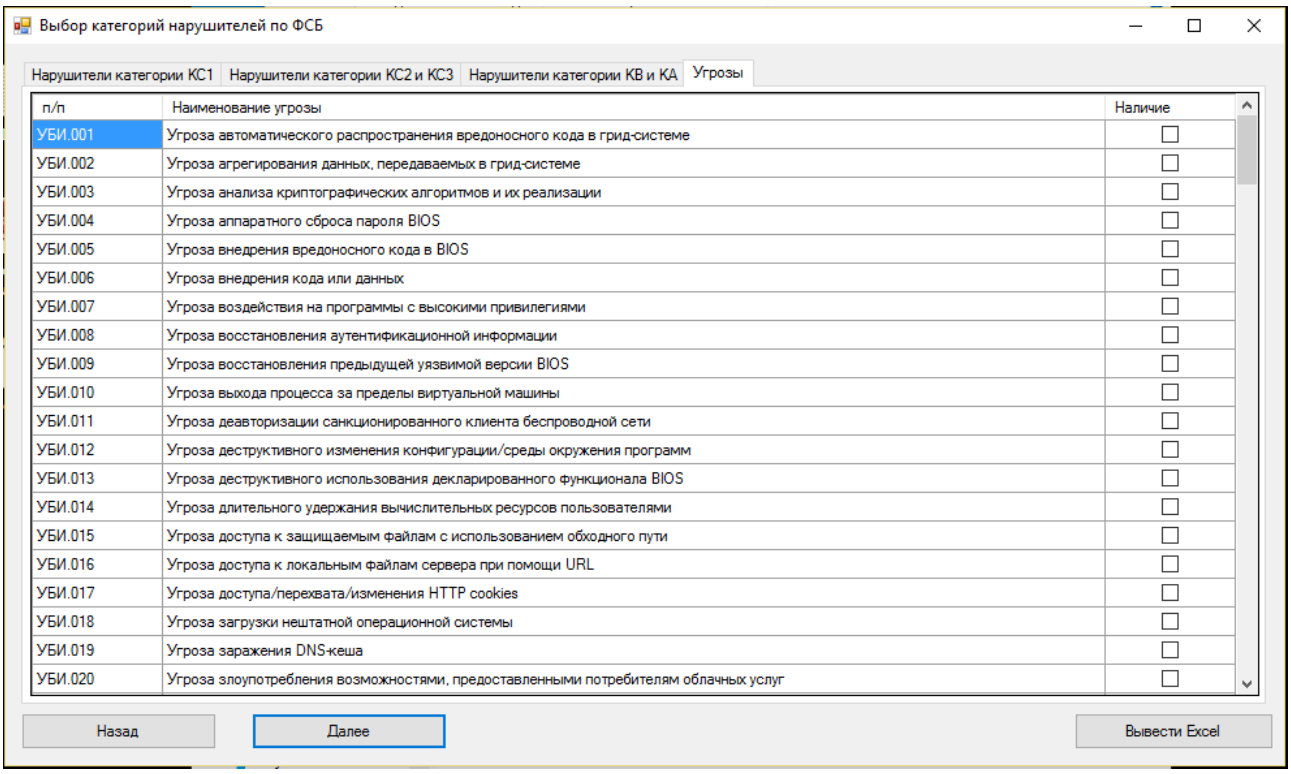

Рисунок 3 - Определение угроз безопасности информации

Если на первом шаге была выбрана информационная система без СКЗИ, то построение модели нарушителя станет производиться по методологии ФСТЭК. (рисунок 4)[2].

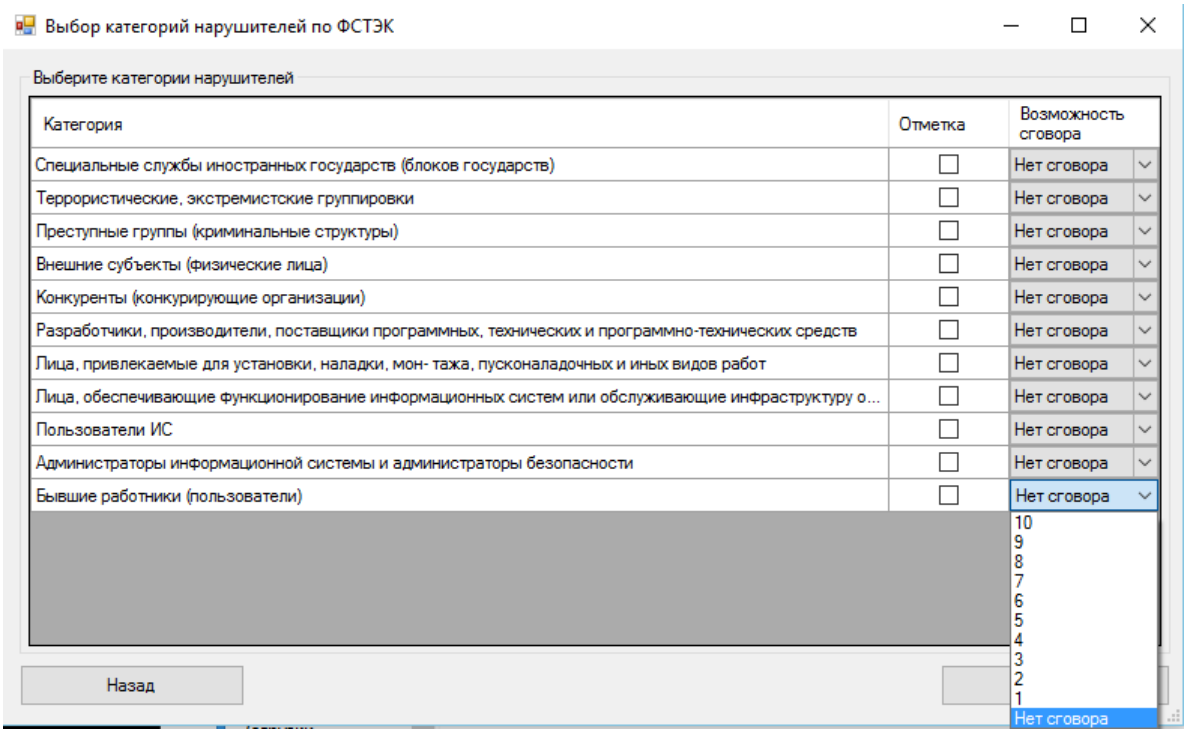

Рисунок 4 – Выбор категорий нарушителя по ФСТЭК

Кроме самих категорий нарушителя имеется пункт «возможность сговора», позволяющий предположить процент сговора нарушителя и сотрудника данной информационной системы.

Конечным шагом в построении модели будет выгрузка полученных данных в Excel. (рисунок 5).

Номер	Наименование нарушителя	Тип нарушителя	Возможные цели Возможные цели (мотивация) реализации угроз безопасности информации	Потенциал нарушителей	Возможные способы реализации угроз безопасности информации	Преднамеренность угроз безопасности	Классификация нарушителей	Возможность сговора
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Нарушители с базовым (низким) потенциалом	УБ5, УБ6	Целенаправленная угроза	Н внешний	Нет сговора
5	Конкуренты (конкурирующие организации)	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием	Нарушители с базовым повышенным(средним) потенциалом	УБ5, УБ6	Целенаправленная угроза	Н внешний	Нет сговора
9	Пользователи ИС	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Нарушители с базовым (низким) потенциалом	УБ3, УБ4, УБ5	Целенаправленная угроза или не целенаправленная угроза	Н2, Н3	Нет сговора
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия	Нарушители с базовым (низким) потенциалом	УБ6	Целенаправленная угроза	Н внешний	Нет сговора

Рисунок 5 – Выгрузка данных в Excel

Подводя итоги вышесказанному, можно сделать вывод о том, что разработка программного модуля уменьшает затраты времени на построение модели нарушителя для ИСПДн, а также позволяет избежать привлечения специалистов по защите информации на этапе предпроектного обследования.

ЛИТЕРАТУРА

1. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

2. Приказ ФСТЭК России от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

REFERENCES

1. Prikaz Federalnoy sluzhby bezopasnosti Rossiyskoy Federatsii ot 10 iyulya 2014 g. N 378 g. Moskva "Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh s ispolzovaniem sredstv kriptograficheskoy zashchity informatsii, neobkhodimykh dlya vypolneniya ustanovlennykh Pravitelstvom Rossiyskoy Federatsii trebovaniy k zashchite personalnykh dannykh dlya kazhdogo iz urovney zashchishchennosti".

2. Prikaz FSTEK Rossii ot 14 fevralya 2008 g. «Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh».

THE PROGRAM MODULE OF CREATION OF MODEL OF THE VIOLATOR FOR PDIS

A.V. VLASENKO, K.V. KLIMENKO, YU.E. EGORIKHIN, E.I. KASHIRINA

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072,
e-mail: Vlasenko@kubstu.ru, elivkashir@yandex.ru

Development of the program module of creation of model of the violator for PDIS, the creation of model of the violator written in the C# language, allowing to automate process according to documents of FSTEC and FSS.

Key words: model of threats, violator's model, PDIS, program module.