УДК 378.147.88/ 004.056

ПРОГРАММНЫЙ КОМПЛЕКС ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ КАК ЭФФЕКТИВНОЕ СРЕДСТВО ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНТНОСТЕЙ БАКАЛАВРОВ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Егорова Ю.Н., Мытникова Е.А., Мытников А.Н., Егорова О.А.

ФГБОУ ВПО «Чувашский государственный университет имени И.Н. Ульянова», Чебоксары, e-mail: amaliaamalia@yandex.ru

В настоящее время обеспечение эффективного противодействия различным угрозам информационной безопасности информационных систем, в том числе от несанкционированного доступа нарушителем, для многих организаций является жизненно важной проблемой. Эта тенденция делает весьма актуальной задачу разработки модели угроз информационной безопасности информационных систем. В работе рассматривается программный комплекс оценки угроз информационной безопасности, который способствует успешному формированию профессиональных компетентностей студентов – бакалавров по направлениям «Прикладная информатика» и «Программная инженерия» на лабораторных работах по дисциплине «Информационная безопасность». Используя программный комплекс, студенты получают реальный опыт работы специалиста в области информационной безопасности. Это поможет им в дальнейшем позиционировать себя как профессионала при устройстве на работу в сферу информационных технологий.

Ключевые слова: информационная безопасность информационных систем, угроза, источник угрозы, оценка угроз, системы защиты информации, модели угроз информационной безопасности, профессиональные компетентности

SOFTWARE INFORMATION SECURITY THREAT ASSESSMENT INFORMATION SYSTEMS AS AN EFFECTIVE MEANS OF FORMATION OF PROFESSIONAL COMPETENCE BACHELOR'S DEGREE IN THE DISCIPLINE «INFORMATION SECURITY»

Egorova Yu.N., Mytnikova E.A., Mytnikov A.N., Egorova O.A.

Federal State Educational Institution «Chuvash State University named after I.N. Ulyanov», Cheboksary, e-mail: amaliaamalia@yandex.ru

Currently providing an effective response to various information security threats to information systems, including the unauthorized intruder, for many organizations is a vital issue. This trend makes it very urgent to develop a model of threats to information security of information systems. In this paper the software package evaluation of information security threats, which contributes to the successful formation of professional competence of students – bachelors on directions «Applied Computer Science» and «Software Engineering» in the laboratory work on the discipline «Information Security». Using the software package, students get real-world experience in the field of information security specialist. This will help them to further position itself as a professional for a job in information technology.

Keywords: information security of information systems, the threat, the source of the threat, threat assessment, protection of information systems, models of information security threats, professional competence

Реалии постиндустриального общества настоятельно требуют повышения уровня информационной подготовки бакалавров, подготавливаемых в системе высшего профессионального образования, обеспечивающего их основные компетенции: общенаучные, инструментальные, профессиональные, социально-личностные и общекультурные. Без них невозможно добиться успехов в реальной жизни в условиях современных рыночных отношений и угроз информационной безопасности, обеспечить конкурентоспособность товаров и услуг, эффективность управления организационных систем любого типа и уровня, реализацию концепции непрерывного самосовершенствования и самообразования личности.

Компетентностный подход при оценке качества подготовки бакалавров заключается в привитии и развитии набора ключевых компетенций, которые определяют его успешную адаптацию в социуме, производственном и научном сообществах. С позиций компетентностного подхода уровень образованности определяется способностью решать задачи различной сложности на основе имеющихся знаний; компетенции, в свою очередь, представляют собой совокупность способностей реализации своего потенциала (знаний, умений, опыта) для успешной производственной и творческой деятельности с учетом понимания проблемы, представления прогнозируемых результатов, вскрытия причин, затрудняющих

деятельность, предложения средств для устранения причин, осуществления необходимых действий и оценки прогнозируемых результатов.

Процесс изучения дисциплины «Информационная безопасность» направлен, прежде всего, на формирование:

– *общекультурных компетенций*: владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения (ОК-1); уметь логически верно, аргументировано и ясно строить устную и письменную речь (ОК-2); стремиться к саморазвитию, повышению своей квалификации и мастерства (ОК-6); осознать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности (ОК-8); использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОК-10); осознать сущность и значение информации в развитии современного общества; владеть основными методами, способами и средствами получения, хранения, переработки информации (ОК-11); иметь навыки работы с компьютером как средством управления информацией (ОК-12); способность работать с информацией в глобальных компьютерных сетях (ОК-13);

– *профессиональных компетенций:* осваивать методики использования программных средств для решения практических задач (ПК-2); разрабатывать интерфейсы «человек – электронно-вычислительная машина» (ПК-3); разрабатывать модели компонентов информационных систем, включая модели баз данных (ПК-4); разрабатывать компоненты программных комплексов и баз данных, использовать современные инструментальные средства и технологии программирования (ПК-5); обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности (ПК-6); готовить презентации, научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и докладов на научно-технических конференциях (ПК-7); участвовать в настройке и наладке программно-аппаратных комплексов (ПК-9).

В статье предлагается программный комплекс, который можно использовать как одно из средств по формированию вышеперечисленных профессиональных компетентностей бакалавров по дисциплине «Информационная безопасность».

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Обеспечение эффективного противодействия различным угрозам информационной безопасности (ИБ) информационных систем, в том числе от несанкционированного доступа нарушителем, является актуальной задачей. Организация обеспечения ИБ информационных систем предполагает оценку значимости угроз.

Угроза (действие) – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации [3].

Источник угрозы – это причины, приводящие к нарушению безопасности информации на конкретном объекте из-за недостатков свойств архитектуры информационной системы, протоколов обмена и интерфейсов, применяемого программного обеспечения и аппаратной платформы, условий эксплуатации [4].

Все источники угроз ИБ можно разделить на три основные группы [2]:

1) источники угроз, обусловленные действиями субъекта (антропогенные источники);

2) источники угроз, обусловленные техническими средствами (техногенные источники);

3) источники угроз, обусловленные стихийными ситуациями.

Полное устранение перечисленных угроз безопасности функционирования информационных систем принципиально невозможно. Проблема оценки угроз ИБ информационных систем состоит в выявлении факторов, от которых они зависят, в создании методов и средств уменьшения их влияния на безопасность функционирования систем [1].

Разработка модели угроз ИБ является одной из основополагающих составных частей при построении системы защиты информации (СЗИ) в организации. Модель угроз представляет собой систематизированный перечень угроз ИБ в информационных системах. Наличие данных угроз обусловлено возможностью осуществления преднамеренного (и/или случайного) воздействия со стороны нарушителя на защищаемую информацию, в результате которого создаются условия или предпосылки для нарушения безопасности информации, приводящее к ущербу жизненно важных интересов личности, общества или государства.

Процесс формирования модели угроз весьма сложен и требует от специалиста высокой квалификации как в теоретической, так и в практической области.

Анализ исследования показал, что основная проблема при разработке модели угроз ИБ – это постоянно увеличивающееся количество защищаемых активов и расплывчатость общепринятых норм оценки рисков и вероятности реализации угроз. В зависимости от вышеперечисленных особенностей актуальность тех или иных угроз ИБ в организации может существенно варьироваться со временем, что требует постоянной доработки и пересмотра сформированной модели угроз. Однако в связи с устоявшимися рыночными отношениями современного общества большинство организаций не готовы выделять ресурсы на осуществление данной деятельности.

По нашему мнению, разработанный нами программный продукт может стать одним из решений вышеназванной проблемы.

В ходе проведения исследования было установлено, что подавляющая часть параметров, влияющих на построение модели угроз, определяется посредством использования метода экспертной оценки, что делает целесообразным применение теории построения экспертных систем при автоматизации данного процесса.

По результатам проведенных исследований была разработана функциональная схема процесса автоматизации формирования модели угроз, представленная на рис. 1.

Блок определения исходного уровня защищенности предназначен для формирования коэффициента ILS, определяющего исходный уровень защищенности. Формирование данного показателя предполагается осуществлять посредством прямого опроса администраторов ИБ организации.

Динамическая база данных содержит перечень необходимой информации, включая сведения о типах и составе защищаемых активов и средств и механизмов защиты информации, совместно с уникальным перечнем атрибутов и метаинформации по каждому конкретному активу и средству защиты информации.

Статическая база данных содержит перечень служебной и справочной информации.

На рис. 2 представлена схема оценки объектов.

Система хранит сведения об объектах защиты, о правилах, о подсистемах. На рис. 3 представлена общая модель работы разработанного программного продукта.

Правило – это набор критериев, которым должен соответствовать объект. В правиле содержится описание правила и методология оценки.

Методология оценки – это описание того, какими способами можно оценить состояние объекта. У каждого объекта есть набор правил, с помощью которых оценивается состояние объекта.

На рис. 4 представлен интерфейс разработанного нами программного комплекса оценки угроз информационной безопасности информационных систем.

Рис. 1. Функциональная схема процесса автоматизации формирования модели угроз безопасности

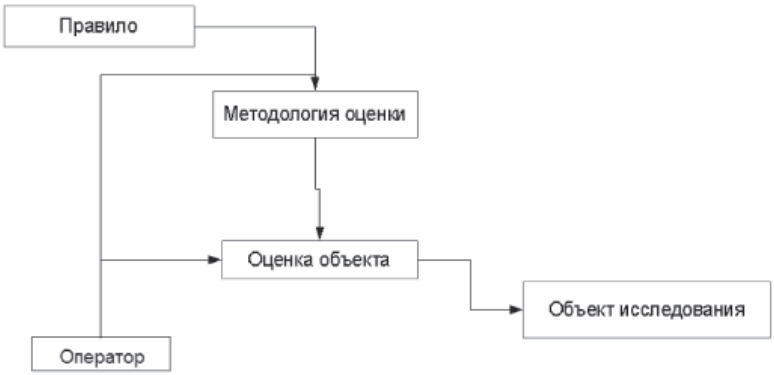

Рис. 2. Схема оценки объектов

Рис. 3. Общая модель работы программы

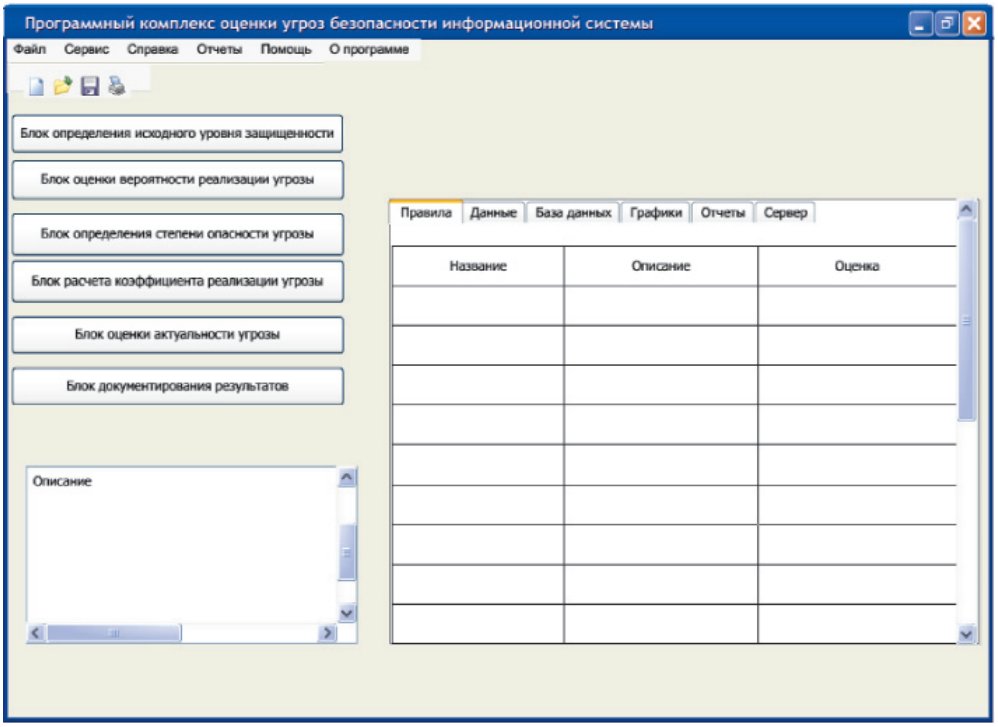

Рис. 4. Интерфейс программного комплекса

Программный комплекс позволяет:

– снизить затраты при обеспечении ИБ в организации;

– практически полностью исключить человеческий фактор (и связанные с ним ошибки) при формировании модели угроз и ее пересмотре;

– увеличить эффективность СЗИ.

Таким образом, можно сделать вывод о том, что разработанный нами программный комплекс оценки угроз информационной безопасности информационных систем можно рассматривать как эффективное средство формирования профессиональных компетентностей бакалавров по дисциплине «Информационная безопасность».

Список литературы

1. Балашов П.А., Кислов Р.И., Безгузиков В.П. Оценка рисков информационной безопасности на основе нечеткой логики // Безопасность компьютерных систем. Конфидент. – 2007. – № 5. – С. 56–59.

2. Биячуев Т.А.. Безопасность корпоративных сетей / под ред. Л.Г. Осовецкого. – СПб.: ГУИТМО, 2006. – 161 с.

3. Брюс Шнайер. Секрети и ложь // Безопасность данных в цифровом мире. – СПб.: Питер, 2003.

4. Егорова Ю.Н. Информационная безопасность: учеб. пособие. – Чебоксары: Изд-во Чуваш. ун-та, 2014. – 69 с.

5. Егорова Ю.Н., Мытников А.Н., Мытникова Е.А., Егорова О.А. Разработка системы управления информационными рисками // Информационные технологии, в экономике, образовании и в бизнесе: VIII материалы Международной научно-практической конференции. (16 декабря 2014 г.); отв. ред. А.А. Зарайский. – Саратов: Издательство ЦПМ «Академия бизнеса», 2014. – С. 40–45.

6. Егорова Ю.Н., Егорова О.А. О некоторых вопросах системы управления информационной безопасностью // Информационные технологии, в экономике, образовании и в бизнесе: материалы Международной научно-практической конференции. (30 сентября 2014 г.); отв. ред. А.А. Зарайский. – Саратов: Издательство ЦПМ «Академия бизнеса», 2014. – С. 40–44.

7. Егорова Ю.Н., Егорова О.А. Проблема обеспечения информационной безопасности геоинформационных систем // Современное образование: актуальные проблемы профессиональной подготовки и партнерства с работодателем: материалы Международной научно-методической конференции. – Томск: Томский гос. ун-т упр.и радиоэлектроники, 2014. – С. 147–149.

8. Мытников А.Н. Модели системы управления информационной безопасностью: маг. дис. – Чебоксары, 2015. – 132 с.

9. Мытникова Е.А. Программный комплекс оценки угроз безопасности информационной системы: маг. дис. – Чебоксары, 2015. – 110 с.

10. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: монография. – М.: Норма, 2004.