РАЗРАБОТКА И ПРИМЕНЕНИЕ СРЕДСТВА АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ УРОВНЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ПОДГОТОВКЕ БУДУЩИХ БАКАЛАВРОВ

Бардукова Н.М., Рычкова А.А.
Оренбургский государственный университет, г. Оренбург

В соответствии с ФГОС ВПО по направлению подготовки 090900 «Информационная безопасность» одной из основных профессиональных задач, связанных с эксплуатационной деятельностью бакалавра является участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации. В процессе обучения в вузе необходимо сформировать соответствующую профессиональную компетенцию – «способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6) » [1].

В результате анализа основных стандартов информационной безопасности автоматизированных систем (АС), средств вычислительной техники(СВТ) и персональных данных (ПДн) нами были выделены основные параметры для сравнения современных стандартов на основе которых проводится оценка защищённости информационных систем [2-10] (таблица 1)

Таблица 1 – Характеристика основных стандартов в сфере оценки информационной безопасности

Критерий сравнения/ Стандарт	ISO/IEC 15408 (ГОСТ Р ИСО/МЭК 15408)	Руководящий документ			«Оранжевая книга»
		«АС»	«СВТ»	«ПДн»	
1	2	3	4	5	6
Год создания	1999 (2002)	1992	1992	1992	1985
Использование	Международный	Только для РФ	Только для РФ	Только для РФ	Только для США
Уровни разделения	Общий уровень доверия (ОУД)	Группы и классы	Классы	Уровни	Уровни и классы
Количество уровней	7 ОУД	3 группы 9 классов	6 классов	4 уровня	4 уровня, 6 классов

Официально признаваемой оценкой защищенности информационных систем (ИС) являются классы защищенности, описание которых приведено в соответствующих стандартах.

Рассмотренные в стандартах подходы обладают рядом недостатков:

– при наличии большого числа стандартов отсутствует единая терминология, которая отслеживает изменения в области защиты информации;

– предъявляются только требования по составу и проведению сертификации средств защиты информации, но отсутствуют количественные показатели и единые требования к функционированию средств защиты информации [11].

Результаты оценки уровня защищённости системы могут применяться при проведении аттестационных и сертификационных испытаниях, а также для повышения уровня защиты имеющейся системы, в случае, если имеющегося уровня не достаточно.

Целью исследования является разработка и применение в учебном процессе такого средства обучения, которое позволит сформировать соответствующую профессиональную компетенцию, необходимую для проведения аттестационного процесса объектов защиты в будущей профессиональной деятельности.

Оценка уровня защищённости информационных систем обычно производится не только на этапе аттестационных испытаний системы для выдачи ей акта соответствия какому-либо классу защиты, но и при лицензировании деятельности предприятия или при проведении сертификационных испытаний для подтверждения соответствия системы какому-либо стандарту, являющимся авторитетным среди экспертов по безопасности.

Существует три типа методов оценки уровня защищённости: экспертный, инструментальный и смешанный (комплексный).

В большинстве случаев процесс оценки производится первым методом, т.е. вручную самим экспертом. Он собирает данные о системе, анализирует, сверяется с руководящими документами или стандартами, а затем выносит решение о принадлежности системы к тому или иному класса защиты и, если требуется, даёт рекомендации для повышения имеющегося уровня. Этот процесс занимает достаточно много времени и является, несомненно, рутинным для специалиста по оценке.

Инструментальное оценивание занимает меньше времени, позволяет более глубоко заглянуть в архитектуру системы, узнать тонкости её функционирования, и, как следствие, дать более полную оценку о существующих уязвимостях системы. Но данный метод имеет ряд недостатков:

– инструментальные средства обычно направлены на сканирование уязвимости какого-либо сегмента системы;

– отсутствие сертифицированных средств для оценки уровня защищённости АС, СВТ и ПДн.

Смешенный метод оценки включает в себя комплексный подход к данному процессу. Он предусматривает как экспертное оценивание, так и инструментальное. Данный метод предоставляет наиболее полную картину об оцениваемой системе: уровень её защищённости в соответствии с руководящими документами, экспертное мнение о подсистемах исследуемой

системы, список уязвимостей системы, многоаспектные рекомендации по повышение уровня защищённости.

Аттестация объектов информатизации по требованиям безопасности информации (обязательная и добровольная) предшествует вводу объекта информатизации в постоянную эксплуатацию и вызвана необходимостью подтверждения соответствия системы защиты информации объекта информатизации требованиям безопасности информации. Процедура аттестации объектов проводится с использованием соответствующих документов [12-13].

Но следует отметить, что процедура аттестации объектов включает в себя целый ряд этапов, например:

– анализ исходных данных;

– проведение экспертного обследования объекта информатизации и анализ имеющейся документации по защите информации объекта на факт ее соответствия требованиям нормативной и методической документации РФ;

– проведение аттестационных испытаний по каждой из систем, находящихся на объекте и т.д.

При проведении испытаний аттестационных систем необходимо установить уровень защищённости данной системы и проверить, является ли он достаточным для обработки информации, которая хранится в данной информационной системе.

Для повышения достоверности оценки уровня защищенности необходимо автоматизировать данный процесс. Нами был проведен сравнительных анализ существующих аналогичных разработок (таблица 2).

Таблица 2 – Сравнительная характеристика средств оценки

Параметр сравнения/ средство оценки	CONDOR+	COBRA	REDCHECK
1	2	3	4
Производитель	Digital Security (Россия)	C & A Systems Security Ltd (Великобритания)	Алтекс СОФТ (Россия)
Стандарт оценки	ISO 17799	ISO 17799	ГОСТ Р ИСО/МЭК 17799, ISO/IEC 27002
Язык интерфейса	Русский	Английский	Русский
Предоставление отчёта	+ (PDF, JPEG, WMF)	+ (MS Office)	+ (PDF)
Метод оценки	Комплексный	Комплексный	Комплексный
Стоимость	225$ и 345$ (с модулем анализа рисков	895 $ и 1995$ (с модулем анализа рисков базового уровня)	33$ (за год) + 23$ (Медиа-комплект для сертифицированно

	базового уровня)		й версии средства анализа защищенности)
Наличие демо-версии	+	-	+

Рассмотренные программные средства обладают рядом недостатков:

1. Данные средства оценки не учитываю ряд руководящих документов Федеральной службы по техническому и экспертному контролю (ФСТЭК);
2. Средства не дают однозначного определения класса для АС или СВТ;
3. Ни одно из средств не классифицирует ИС для обработки ПДн;
4. Все средства являются платными.

Проведенный анализ свидетельствует о необходимости разработки собственного программного средства для оценки уровня защищенности информационных систем.

На рисунке 1 представлена укрупненная схема авторского алгоритма разрабатываемой программы.

Рисунок 1 – Структурная схема алгоритма программы

Процесс проведения оценки уровня защищенности является циклическим, а достижение желаемого или требуемого уровня защищённости иногда происходит в несколько этапов поиска решений.

Для повышения уровня защищённости системы на 7 шаге алгоритма могут использоваться следующие меры:

1. Использование дополнительных организационных и технических средств защиты;

2. Изменение архитектуры или схемы информационных потоков ИС, что позволяет повысить уровень защищённости системы (например, физическое отключение от сети интернет сегмента ИС, в котором обрабатываются ПДн).

Обычно повышение уровня безопасности направлено лишь до определённого уровня, который устраивает руководителей организации и удовлетворяет всем стандартам и законодательству РФ. При выборе мер по повышению уровня защиты АИС учитывается одно принципиальное ограничение: стоимость их реализации не должна превышать стоимость защищаемых информационных ресурсов.

В завершение процедуры, результаты оценки оформляются в виде отчётного документа, который предоставляется руководству организации. В документ обычно включаются следующие разделы:

1. Описание границ, в рамках которых была проведена оценка безопасности.

2. Описание структуры информационной системы ПДн.

3. Методы и средства, которые использовались в процессе проведения оценки уровня защищённости.

4. Описание выявленных несоответствий (в случае оценки на соответствие законодательству) или список актуальных по мнению экспертов угроз.

5. Рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности.

6. Предложения по плану реализации мер, которые приведут к желаемому уровню защищённости системы.

Таким образом, разрабатываемое программное средство автоматизированной оценки уровня защищенности информационных систем позволит будущим бакалаврам выступить в роли экспертов при проведении аттестационных процедур, применить и закрепить полученные теоретические знания в области аттестации на конкретном примере, а также выявить возможные пробелы в знаниях и устранить их.

Список использованных источников

1. Федеральный государственный стандарт высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) "бакалавр". - Приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. N 496

2. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 1992. – 13 с.

3. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации / Государственная техническая комиссия при Президенте Российской Федерации. 25 июля 1997 г.;

4. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации / Государственная техническая комиссия при Президенте Российской Федерации. 30 марта 1992 г.;

5. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации / Государственная техническая комиссия при Президенте Российской Федерации. 30 марта 1992 г.;

6. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники / Государственная техническая комиссия при Президенте Российской Федерации. 30 марта 1992 г.;

7. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. - Часть1. Введение и общая модель. – Госстандарт России, Москва, 2002.

8. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Госстандарт России, Москва, 2002.

9. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Госстандарт России, Москва, 2002.

10. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных / ФСТЭК России. 15 февраля 2008 г. ФСТЭК;

11. Оценки защищённости информационных систем. / [Эл. ресурс] – Точка доступа: http://jurnal.org/articles/2008/inf33.html. *– Режим доступа: свободный.*

12. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.);

13. Национальный стандарт Российской Федерации ограниченного распространения ГОСТ РО 0043-003-2012 «Защита информации. Аттестация

объектов информатизации. Общие положения» (принят и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 17.04.2012 г. № 2-ст РО).