УДК 004.056

Оксиюк А. Г., доктор техн. наук, доцент. Тел.: +380 (67) 466 82 94. E-mail : oksiuk@ukr.net
Шестак Я. В., аспирантка. E-mail : lucenko.y@ukr.net
(Киевский национальный университет имени Тараса Шевченко)

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДИК И МЕТОДОВ ПРОВЕДЕНИЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Oksiyuk O. H., Shestak Ya. V. Analysis of modern methodologies and methods for assessing the security of information systems. The article is devoted to an actual problem of information systems' security assessment and the importance of objective quantitative assessment results receiving. The author offers the creation of complex system of information security with system approach, which will be used at each stage of information system's life cycle. On the basis of this approach the author formulates the general scheme of an information security assessment of information system, and also the principles of an assessment's carrying out method choice. In this work the existing methods of a quantitative assessment based on object-oriented methods of the system analysis, and also the objectivity of the received estimates on the basis of this approach are considered. On the basis of the carried-out analysis, serious shortcomings of the used modern techniques of an information systems' security assessment are allocated, then the idea of the scientific and methodical device providing the increase of objectivity and complexity of an information assessment means on the basis of expert data formalization creation necessity was formulated.

Keywords: information system, assessment methods, information protection, system analysis

Оксіюк О. Г., Шестак Я. В. Аналіз сучасних методик та методів проведення оцінки захищеності інформаційних систем. На основі запропонованого підходу підходу формується загальна схема оцінки захисту інформації в інформаційній системі, а також принципи вибору методу проведення оцінки. У роботі розглянуті існуючі методи кількісної оцінки, засновані на об'єктно-орієнтованих методах системного аналізу, а також об'єктивність отримуваних оцінок на основі цього підходу. На основі проведеного аналізу виділені серйозні недоліки використовуваних сучасних методик оцінки захищеності інформаційних систем, була сформована ідея про необхідність створення науково-методичного апарату, що забезпечує підвищення об'єктивності і комплексності оцінки засобів захисту інформації на базі формалізації експертних даних.

Ключові слова: інформаційна система, методи оцінки, захист інформації, системний аналіз

Оксиюк А. Г., Шестак Я. В. **Анализ современных методик и методов проведения оценки защищенности информационных систем**. На основе предложенного системного подхода сформулирована общая схема оценки защиты информации в информационной системе, а также принципы выбора метода проведения оценки. В работе рассмотрены существующие методы количественной оценки, основанные на объектно-ориентированных методах системного анализа, а также объективность получаемых оценок на основе данного подхода. На основе проведенного анализа выделены серьезные недостатки используемых современных методик оценки защищенности информационных систем, была сформулирована идея о необходимости создания научно-методического аппарата, обеспечивающего повышение объективности и комплексности оценки средств защиты информации на базе формализации экспертных данных.

Ключевые слова: информационная система, методы оценки, защита информации, системный анализ

Вступление. На сегодняшний день одной из важнейших глобальных проблем в области информационных технологий является задача обеспечения информационной безопасности электронных ресурсов от несанкционированного проникновения. Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая представляет собой совокупность инфраструктуры и субъектов, осуществляющих сбор, формирование и распространение информации. Интенсивное развитие и широкое применение информационных технологий во всех сферах человеческой деятельности является объективным фактором, определяющим проблему обеспечения информационной безопасности как одну из наиболее важных.

В связи с широким распространением глобальной информационной сети Интернет и развитием компьютерных сетей возникла потребность в защите компьютеров от внешних воздействий со стороны злоумышленников. Осуществление атак через сеть Интернет становится мощным средством проведения информационных операций, а также совершения преступлений в финансовой и других сферах. Современные компьютерные системы являются территориально распределенными компьютерными сетями, объединяющими с помощью каналов связи различные компьютеры и локальные сети. Уязвимость распределенных вычислительных систем существенно превышает уязвимость автономных компьютеров. Это связано, прежде всего, с открытостью, масштабностью и неоднородностью самих компьютерных сетей. Соответственно существует немало способов атак на современные компьютерные сети. При этом количество угроз компьютерной безопасности и способов их реализации постоянно увеличивается. Основными причинами здесь являются недостатки современных информационных технологий, а также неуклонный рост сложности программно-аппаратных средств.

Значимость проблемы защиты информации в современном мире является признанной, и подтверждение этому являются понесенные корпорациями огромные убытки из-за недостаточной защищенности информации. Однако, проведённый анализ в области нарушений безопасности информации указывает на наличие серьёзных трудностей, которые во многом связаны с отсутствием единой системы оценки защищенности информации, позволяющей дать количественную оценку, при проектировании и эксплуатации информационных систем.

Общая методика построения систем защиты информации. В настоящее время на рынке защиты информации предлагается много отдельных инженерно-технических, программно-аппаратных, криптографических средств защиты информации.

Решение проблемы, возникающие при защите информации в автоматизированных информационных системах (АИС), является сложным процессом, который базируется на основе системного подхода, применяемого при создании комплексной системы защиты информации.

Для обеспечения защищенности информации в АИС крайне важно использование мероприятий, направленных на защиту информации на всех этапах жизненного цикла АИС.

Жизненный цикл можно разделить на четыре этапа [1]:

– проектирование;
– ввод в действие;
– эксплуатация;
– сопровождение.

На первом этапе жизненного цикла АИС необходимо произвести идентификацию рисков для системы и выявить недопустимые риски, которые необходимо уменьшить или удалить средствами защиты АИС. После чего, ответственное лицо анализирует ожидаемые остаточные риски и принимает решение об их приемлемости для проектируемой АИС.

Следующим шагом на этапе проектирования АИС является выбор аппаратного обеспечения, программных продуктов, обеспечивающей инфраструктуры, прикладного программного обеспечения и необходимых технических средств регулирования безопасности АИС. На данном этапе уже следует производить оценку безопасности, проектируемой АИС. Это позволит специалистам по обеспечению защищенности АИС дать понимание устройства системы, а также ее предполагаемой эксплуатационной среды.

После анализа внешней и внутренней среды функционирования АИС идет закупка базового и прикладного программного обеспечения, а также технические инструменты

регулирования безопасности. Параллельно с этим создается инфраструктура безопасности для административного и процедурного уровней, с полным документированием политик, правил и процедур безопасности, интегрируемые в систему защиты АИС.

В случае внесения изменений в существующую автоматизированную информационную систему, то должна выполняться замена технических средств регулирования безопасности в соответствии с изменившейся средой.

Следующий шаг – оценка автоматизированной информационной системы. Это позволяет владельцу АИС получить независимое подтверждение того, что все выявленные риски благодаря применению средств регулирования безопасности сведены до приемлемого уровня. Проведение оценки необходимо для проверки АИС на соответствие к предъявляемым к ней системным требованиям. Как правило, специфические параметры безопасности, характерные для конкретной организации (административные, технические и т.д.), могут быть установлены до начала ввода в эксплуатацию автоматизированной информационной системы. Результатом первого этапа является подтверждение приемлемости существующих угроз безопасности для функционирования АИС в производственной среде и возможности ввода системы в эксплуатацию.

На втором этапе происходит развертывание и инсталляция автоматизированной информационной системы, подготовка к эксплуатации.

На этапе эксплуатации выполняется непрерывное протоколирование и отслеживание работы технических, процедурных и административных средств регулирования безопасности. Реализуется обратное взаимодействие для корректировки средств регулирования безопасности при внесении изменений в АИС. Обеспечение обратного взаимодействия с АИС проводится мониторинг не всех средств регулирования безопасности, а наиболее важных критериев подмножеств, сгруппированных на логическом подходе. Для реализации возможности мониторинга АИС у администратора должна быть возможность управления конфигурацией, аудита и администрирования.

Этап сопровождения связан с анализом всех предложенных или сделанных изменений в АИС, конфигурации средств регулирования безопасности, включая изменения в правилах, процедурах и политиках. Данный этап завершается выведением системы из использования и перемещением данных в другую систему или перемещением в долговременный архив. Ответственное лицо должно потвердить факт успешного завершения работы АИС.

Учитывая особенности организации защиты информации на всех этапах жизненного цикла построения системы защиты АИС можно выделить следующие этапы [2]:

– разработка профилей защиты (ПЗ) для АИС, формирование совокупности требований к безопасности и спецификаций, включенных в профиль защиты АИС;

– разработка методов оценки реализации ПЗ;

– проведение оценки ПЗ на полноту, непротиворечивость и достаточность требований к параметрам безопасности.

– проведение комплексной оценки реализации задачи безопасности;

– ведение мониторинга эффективности применяемых мер по обеспечению безопасности информации.

Наиболее важным этапом при построении комплексной системы защиты информации является этап оценки систем защиты информации АИС.

Общая схема оценки приведена на Рис. 1.

При проведении оценки систем защиты информации АИС основными вопросами являются:

– отвечает ли функция безопасности АИС требованиям, указанным в ПЗ;

– корректно ли реализована функция безопасности АИС.

При выборе метода оценки защищенности информации необходимо придерживаться следующих принципов:

объективность – результаты оценки должны быть основаны на фактических данных и не зависеть от личного мнения;

воспроизводимость – при использовании одних и тех же входных данных для оценки должен всегда приводить к идентичным результатам;

корректность – случайные действия оценивающего не должны оказывать действия точность оценки;

достаточность – действия по оценке проводятся до уровня, требуемого для удовлетворения заданного критерия доверия.

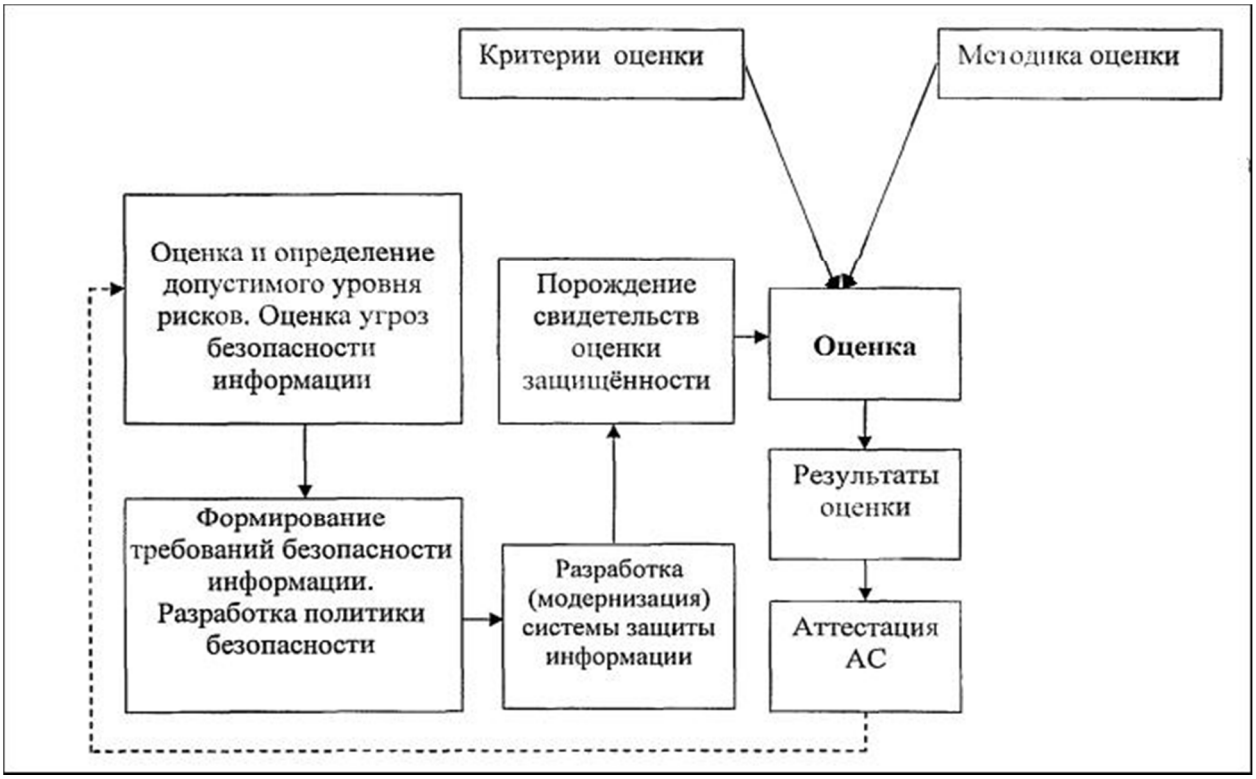

Рис. 1. Процедура оценки системы защиты информации АИС

Для проведения оценки состояния системы защиты информации АИС необходимо проводить анализ всей структуры требований безопасности, состоящих из совокупности частных показателей подмножеств, сгруппированных на основе логического подхода [2, 3].

Данный процесс можно представить в виде следующе последовательности этапов:

- процедура нечеткого экспертного оценивания элемента (частные показатели подмножеств);
- процедура нечеткого оценивания показателей совокупности подмножеств, на основе эвристических методов представления экспертных оценок;
- процедура определения весов важности показателей;
- процедура получения оценки в соответствии с иерархической структурой показателей.

Современные методы оценки системы защиты информации (СЗИ). Развитие научного направления в области оценки защищенности информации в информационной системе, с использованием систем защиты информации, осложняется отсутствием единой системы понятий и категорий для оценки СЗИ [4].

Оценка защиты информации в АИС строится на основе подхода, смысл которого заключается в присвоении АИС определенного класса защиты, исходя из степени реализованных в ней типовых конфигураций средств защиты информации и организационных мероприятий. На сегодняшний день данный подход используется во всех современных нормативных актах, как в иностранных, так и в украинских.

Проведенный анализ наиболее распространенных методик в области оценки защищенности АИС позволяет выделить три основных метода оценки защищенности АИС:

– формальный;
– статистический;
– классификационный.

Не получил большого практического применения формальный метод оценки защищенности АИС ввиду сложности в формализации основных понятий: сопротивляемость механизма защиты, угрозы безопасности и ущерба от реализации угрозы безопасности.

Статистический подход, в свою очередь, основывается на сборе и накоплений статистики о частоте возникновениях инцидентов в АИС и расчете на их основе статистических вероятностей возникновения соответствующих угроз. На практике получить реальные данные, используя статистический подход, практически невозможно. Это связано с трудностью сбора информации по событиям, вероятность происшествия которых крайне мала, а также с тем, что система не является статичным объектом, а находится в стадии постоянного развития, в рамках которого происходит изменение в составе программного, аппаратного обеспечения и СЗИ. В связи с трудностью постоянного сбора статистической информации в рамках изменяемой информационной системы, статистический подход при оценке защищенности применим лишь частично, как дополнительное средство при наличии достоверной статистической базы.

На практике большое применение получил неформальный классификационный подход с применением неформальных моделей защиты АИС, в качестве значений показателей объектов которых используется их отнесение к определенным категориям. Данный подход не дает получить точное значение показателя защищенности, но позволяет классифицировать и сравнивать АИС по уровню защищенности. Для оценки степени реализации механизмов регулирования безопасности используют методы активного и пассивного тестирования системы защиты информации. Для этого проводят имитацию действий потенциального злоумышленника по преодолению механизмов и средств защиты, или применяют списки проверки и о анализируют конфигурацию устройств, операционные системы и приложения. Тестирование может проводиться как вручную, так и с использованием специализированного программного обеспечения.

В качестве примера указанного программного обеспечения является семейство продуктов компании Internet Security Systems, включающее следующие подсистемы:

– анализ защищенности уровня ОС – System Scanner;
– анализ защищенности уровня СУБД – Database Scanner;
– анализ защищенности уровня ЛВС – Internet Scanner;
– анализ защищенности уровня радио сетей – Wireless Scanner.

Механизм автоматизации процесса оценки защищенности информации во всех существующих методах базируется на применении технологии баз данных, с разделением на количественные и качественные.

Ввиду относительной простоты качественные методики оценки защищённости получили наиболее широкое применение. Разработано достаточно большое количество методик, которые базируются на использование различных средств автоматизации. Одними из наиболее известных методик являются: COBRA, RA Software Tool и MethodWare [5].

Данные методики позволяют жать оценку соответствия системы безопасности организации международным стандартам или иным стандартам безопасности [6]. Оценки производятся с использованием качественных шкал на основе данных, полученных с использованием тематических опросников.

Существующие количественные методы оценки используют объектно-ориентированные методы системного анализа. Для проведения оценки используют базы данных уязвимостей, а также иные сложные инструментальные средства. К данным методикам можно отнести CRAMM [4, 7], RiskWatch [5], и «Гриф» и «АванГард» [8]. Проведенный анализ подобных методик показывает, что в качестве количественных данные методики могут быть использованы весьма условно, т.к. полученные бальные результаты являются весьма субъективными и не лучше качественных шкал. На основе вышесказанного можно утверждать, что в настоящий момент основным подходом для оценки средств защиты информации АИС является классификационный подход. Данный подход использует шкалу интервалов значений, которая позволяет получать числовые оценки ключевых параметров путем их категорирования и соотношения с некими значениями, используемыми в конкретном методе оценки защищенности информации.

К серьезным недостаткам используемых в современных методиках оценки защищенности АИС необходимо отнести малоэффективное применение знаний экспертов. При проведении оценки ограничиваются получением точных оценок выбранных ключевых показателей, а также серьёзным недостатком является отсутствие комплексности получаемых оценок. Проведение оценки СЗИ АИС на основе большинства современных методик характеризуется высокой трудоемкость.

Таким образом, используемые современные методики оценки средств защиты информации АИС обладают рядом существенных недостатков, затрудняющих их практическое применение и снижающих ценность получаемых с их помощью результатов. Проведенный анализ показал, что на текущий момент не существует методик и методов оценки СЗИ АИС, удовлетворяющие современным требованиям по объективности, комплексности и трудоемкости оценки.

Постановка задачи оценки СЗИ. Проведенный анализ современных методик и методов проведения оценки СЗИ АИС выявил несоответствие между необходимостью получения объективных количественных данных по оценке СЗИ АИС и невозможности получения их современными методами. Данное противоречие не позволяет реализовать заданный уровень защищенности АИС, при обеспечении эффективности их использования в условиях развития АИС, появления новых уязвимостей и угроз, а также затраты средств, предоставляемых на решение данной задачи при отсутствии реальных данных о функционировании СЗИ.

Для решения данной проблемы можно использовать методики и методы, поддерживающие автоматизированные средства, обеспечивающие повышение объективности и оперативности оценки защищенности АИС на основе применения методов построения прогностических моделей, мониторинга потенциально опасных объектов, формализации экспертной информации с целью создания методологической основы [3, 9].

Следовательно, для дальнейшего повышения точности результатов анализа СЗИ требуется:

- разработка модели оценки СЗИ АИС, которая позволит учитывать аспекты трудно формализуемых данных предметной области.
- разработка методики оценки защищенности АИС, а также поддерживающие автоматизированные средства, обеспечивающие повышение объективности и оперативности оценки защищенности АИС.

Проведенный анализ позволяет выдвинуть идею о необходимости создания научно-методического аппарата, обеспечивающего повышение объективности и комплексности оценки средств защиты информации на базе формализации экспертных данных. Внедрения в практику методики и модели оценки СЗИ АИС позволит повысить защищенность АИС и её отдельных компонентов.

Разрабатываемая модель оценки должна позволить с высокой степенью объективности проводить оценку СЗИ АИС, как совокупности элементов, её составляющих, по трем аспектам – сохранения целостности, доступности и конфиденциальности информации.

Выводы. Проведенный анализ современных тенденций к оценке защищенности АИС показывает, что включенные в него подходы, методы, методики и средства анализа СЗИ АИС являются наиболее важными и отражают основные направления исследований в данной области, а также позволяет выделить следующие противоречия:

– требования руководящих и нормативных документов в области защиты информации носят разрозненный характер, и не охватывают все аспекты защиты информации в современных АИС.
– несоответствие моделей функционирования СЗИ современных АИС и методов проведения оценки не соответствуют современным требованиям оценки защищенности.
– активное увеличение числа АИС, делает невозможным участия ведущих экспертов по защите информации при разработке и внедрения АИС.

В работе рассмотрены современные подходы к оценке СЗИ АИС, сформулирована общая методика оценки СЗИ АС, а также сформулирована постановка задачи оценки СЗИ АИС.

Литература

1. Галатенко В. А. Оценка безопасности автоматизированных систем. Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 197911. Jet Info online! / В. А. Галатенко // Информационный бюллетень. – 2005. – №7.

2. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – Санкт-Перербург : БХВ-Петербург, 2003. – 752.

3. Бойченко О. В. Модель корпоративного інформаційного захисту об'єкту інформатизації / О. В. Бойченко, Я. І. Торошанко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №4(20). – С. 15-19.

4. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – Санкт-Перербург : Наука и техника, 2004. – 384 с.

5. Касперский Е. В. Компьютерное зловредство / Е. В. Касперский. – Санкт-Перербург : Питер, 2007. – 208 с.

6. Столингс В. Основы защиты сетей. Приложения и стандарты ; пер с англ. / В. Столингс. – Москва: Изд. дом «Вильямс», 2002. – 432 с.

7. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян. – 2-е изд. – Санкт-Перербург : БХВ-Петербург, 2003. – 368 с.

8. Бурдин О. А. Комплексная экспертная система управления информационной безопасностью «АванГард» / О. А. Бурдин, А. А. Кононов // Информационное общество. – 2002. – №3. – Вып. 1. – 38 с.

9. Кравченко Ю. В. Концепція структурування інформаційного ресурсу системи дистанційного навчання / Ю. В. Кравченко, О. Г. Оксіюк // Сучасні інформаційні технології у сфері безпеки та оборони. – 2009. – №1 (4). – С. 6-11.

Дата надходження в редакцію: 22.07.2015 р. Рецензент: д.т.н., проф. Ю. В. Кравченко