УДК: 004.056.53

Толюпа С. В., доктор техн. наук, проф. Тел.. +38(050)773 46 57. E-mail : tolupa@i.ua
Наконечный В. С. доктор техн. наук. Тел.+380 (66) 305 15 85. E-mail: nvc2006@mail.ru
Якименко Ю. М., канд. военных наук. Тел.+380(67) 277 22 20. E-mail: yakimenko.um@mail.ru
(Государственный университет телекоммуникаций, г. Киев)

ОЦЕНКА ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ С ПОМОЩЬЮ ОБЩИХ КРИТЕРИЕВ

Tolyupa S. V. Nakonechnyy V. S., Yakymenko Yu. M. Assessment of information security in automated information systems using Common criteria. The various independent methods of estimation of efficiency of functioning of information protection systems do not provide a clear and objective picture of the state automated information system. In world practice there is a search of ways to improve the objectivity of evaluation of information security in the organization, aimed primarily at improving the existing international standards. It is offered to evaluate information security in automated information systems, using Common criteria of information technology security, according to the attached methodological scheme. This allows you to competently perform the evaluation only to clarify or to establish new requirements for information security.

***Keywords*:** information security, automated information system, Common criteria, information protection system, threat, assessment

Толюпа С. В., Наконечний В. С., Якименко Ю. М. Оцінка захищеності інформації в автоматизованих інформаційних системах з допомогою Загальних критеріїв.
Різноманіття різних не взаємопов'язаних методів оцінки ефективності функціонування системи захисту інформації не дозволяє отримати однозначну і об'єктивну картину стану автоматизованої інформаційної системи. Оцінку захищеності інформації в автоматизованих системах обробки інформації пропонується проводити за допомогою Загальних критеріїв оцінки безпеки інформаційної технології за доданою схемою. Це дозволяє грамотно провести не тільки оцінку, а й уточнити або задати нові вимоги до безпеки інформації.

***Ключові слова*:** інформаційна безпека, автоматизована інформаційна система, Загальні критерії, система захисту інформації, загроза, оцінка

Толюпа С. В., Наконечный В. С., Якименко Ю. М. Оценка защищённости информации в автоматизированных информационных системах с помощью Общих критериев.
Многообразие различных не взаимосвязанных методов оценки эффективности функционирования системы защиты информации не позволяет получить однозначную и объективную картину состояния автоматизированной информационной системы**.** Оценку защищённости информации в автоматизированных системах обработки информации предлагается проводить с помощью Общих критериев оценки безопасности информационной технологии по прилагаемой схеме. Это позволяет грамотно провести не только оценку, но и уточнить или задать новые требования к безопасности информации.

***Ключевые слова*:** информационная безопасность, автоматизированная информационная система, Общие критерии, система защиты информации, угроза, оценка

1. Введение и постановка задачи. Отсутствие на сегодняшний день эффективного методического подхода к решению задач защищённости информации, особенно в выборе и учёте требований по безопасности, закономерно влечёт за собой многообразие различных не взаимосвязанных методов оценки эффективности функционирования системы защиты информации. Необходимость проведения дальнейших исследований в поиске эффективных подходов в обеспечении безопасности информации в АИС и её оценки выступает первоочередной актуальной задачей сегодняшнего дня.

2. Анализ литературных данных. В современных условиях наиболее перспективным способом проверки достигнутого качества функционирования и уровня защищенности АС, как отмечается в [1], является процедура её оценки по выполнению требований информационной безопасности (ИБ). Требования безопасности используются в качестве

критерия для оценки уровня защищенности АС или средств вычислительной техники (СВТ). Эти требования могут быть сформулированы в руководящих или нормативных документах.

В соответствии с [2] в зависимости от выбранного критерия предлагаются способы оценки ИБ организации: *оценка по эталону, риск-ориентированная оценка и оценка по экономическим показателям.*

Под *оценкой соответствия ИБ организации установленным критериям* (требованиям *по эталону*) понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации.

Риск-ориентированная оценка ИБ организации представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в информационной сфере организации, сопоставляются существующие риски ИБ и принимаемые меры по их обработке.

Способ оценки ИБ на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования ИБ (в качестве критериев эффективности системы используются показатели совокупной стоимости владения – ТСО).

Перечисленные способы оценки ИБ для организации с АИС могут быть применимы частично, так как связаны в основном с экономическими показателями.

В работе [3] предлагается для оценки качества системы защиты информации в сложных системах использовать международные стандарты ISO/IEC 17799 и ISO/IEC 15408. В первом из них приводятся основы проверки системы на соответствие требованиям информационной безопасности, а также содержатся практические рекомендации.

В стандарте ISO/IEC 15408, как наиболее универсальном и совершенном, представлены механизмы профиля и проекты, отражающие суть концепции решения проблемы защиты информации и определены критерии безопасности информационных технологий. В нём не приводится в готовом виде список требований по безопасности, но положения стандарта позволяют сформулировать цели безопасности, направленные на обеспечение противостояния угрозам, то есть те цели, которые должны использоваться как основа для оценки свойств систем и информационных технологий. Только потом с помощью стандарта могут быть сформулированы требования, а эксперты по безопасности определить, отвечает ли система этим требованиям.

3. Цель и задачи исследования. Потенциальным объектом для нанесения ущерба может служить любая информация, заложенная в компьютерную систему , проходящая по вычислительным сетям или находящаяся на электронных или бумажных носителях и способная принести прибыль злоумышленнику.

Поэтому актуальным для автоматизированной информационной системы организации продолжает оставаться защищенность её от случайного или преднамеренного вмешательства в нормальный процесс функционирования – от попыток хищения, модификации или разрушения ее компонентов.

Обеспечение безопасности информации в АИС можно добиться, прежде всего, за счёт наличия и использования существующих методик её оценки , учитывающих требования государственных законодательных и других нормативных документов по безопасности, выработки требований и оперативного принятия мер по повышению эффективности защиты информации. Рассмотрение этих вопросов и является задачей исследования.

4. Особенности организации защиты информации в АИС. Наиболее перспективными средствами защиты информации в компьютерных системах являются программные средства. Они позволяют создать модель защищенной системы с построением правил разграничения доступа, централизованно управлять процессами защиты и интегрировать различные механизмы в единую систему.

Несмотря на явные преимущества обработки, немало сложностей при организации защиты информации возникает в компьютерных сетях по причине:

– *расширения зоны контроля*: администратором затруднён контроль за деятельностью пользователей в отдельной подсети, находящихся вне пределов его досягаемости;

– *появления неизвестного периметра*: невозможно чётко определить границы сети из-за изменений вследствие её расширения, один и тот же узел может быть доступен для пользователей различных сетей;

– *использования разнообразных программно-аппаратных средств*: – снижение защищённости системы в целом при соединении нескольких систем защиты отдельных сетей в общую сеть, так как каждая система настроена на выполнение своих требований по безопасности и может быть несовместима в требованиях с другими системами;

– *сложности в управлении и контроле доступа к системе*: сложность идентификации нарушителя из-за того, что атаки на сеть, как правило, осуществляются из удаленных точек без физического доступа к определенному узлу;

– *увеличении количества возможных точек атаки*: трудность в их контроле, так как воздействие может происходить на линии связи и различные виды коммуникационного оборудования – через получение доступа с помощью коммутационных средств и модема, тем самым увеличивая возможные источники угроз.

В отношении использования вычислительной техники в АИС в настоящее время необходимо учитывать характерные и типичные следующие особенности [4]: возрастающий удельный вес автоматизированных процедур, нарастающая важность и ответственность принимаемых решений, увеличивающаяся концентрация в АИС информационно-вычислительных ресурсов, большая территориальная распределенность_компонентов АИС и другое.

Исходя из выше приведенного в качестве объектов уязвимости АИС, которые могут привести к негативным последствиям, рассматриваются:

– динамический вычислительный процесс обработки данных, автоматизированной подготовки решений и выработки управляющих воздействий;

– информация, накопленная в базах данных;

– объектный код программ, исполняемых вычислительными средствами в процессе функционирования ИС;

– информация, выдаваемая потребителям и на исполнительные устройства.

5 .Оценка защищённости информации в АИС с помощью Общих критериев. Для оценки защищённости информации в АИС могут быть использованы Общие критерии оценки безопасности информационной технологии (ССЕВ) [5], в разработке которых использован признанный в мировой практике стандарт ISO/IEC 15408, приводятся функциональные требования к безопасности и гарантии оценки, а также содержатся критерии, которые нужно использовать оценщиками при формировании заключений относительно соответствия объектов оценки требованиям безопасности.

Функциональные требования включают требования идентификации, установления подлинности (аутентификации) пользователей, протоколирования (аудита) и другое.

Требования гарантированности сводятся к требованиям по организации процесса разработки и по поиску, анализу и воздействию на потенциально уязвимые места с точки зрения безопасности информации.

В общем виде концептуальная схема оценки безопасности информации в АИС может быть представлена на Рис. 1.

В соответствии со схемой перед оценкой безопасности информации в организации должен быть проведен анализ рисков с использованием модели угроз – выявлены из общего количества угроз наиболее опасные, определены уязвимости и приняты меры по предотвращению возможного ущерба.

Пакет функциональных требований предназначается для многократного использования и определяет те требования, которые являются необходимыми для достижения выбранных целей. Функциональные требования включают: требования идентификации и аутентификации, требования аудита, требования администрирования, требования управления доступом, защиту функций безопасности и посредничество ссылок.

Уровень гарантированности – это набор базовых требований гарантии для оценки безопасности, который обеспечивается независимым испытанием и анализом функций безопасности оцениваемой системы, подкреплённым документами разработчика: актом испытаний и свидетельством поиска явных уязвимых мест на проектной стадии системы.

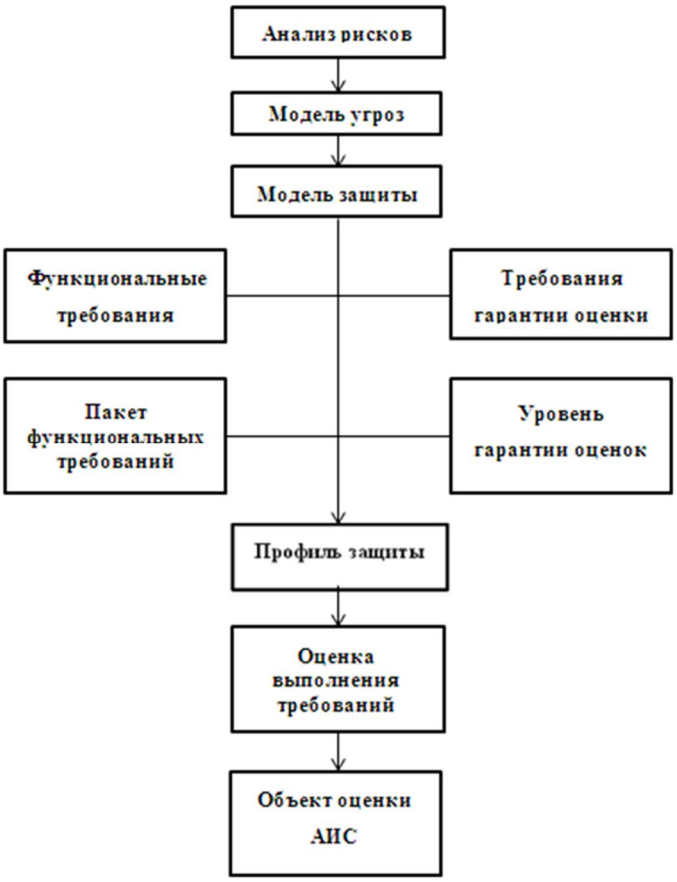

Рис. 1. Концептуальная схема оценки безопасности информации в АИС

Профиль защиты предназначен для многократного использования и определяет совокупность требований безопасности к оцениваемой системе, которые являются необходимыми и эффективными для достижения поставленных целей.

Профиль состоит из следующих частей:

1. Безопасность окружающей среды – описание проблемы безопасности, которая должна быть решена. Окружающая среда описана в терминах ожидаемых угроз, политики безопасности, которая должна быть предписана, и условий использования оцениваемой системы.

2. Цели безопасности – совокупность формулировок, подводящих итог решаемой задачи безопасности и являющихся базисом для определения требований.

3. Функциональные требования – эти требования включают функции безопасности различного уровня детализации, поддержанные компонентами аудита безопасности семейства. Запись аудита может предусматривать действия, которые раскрываются в терминах: *минимальный* – успешное использование механизма безопасности; *базовый* – любое использование механизма безопасности, включая использование информации признаков безопасности; *детализированный* – контроль любых изменений конфигурации

механизма безопасности, включая оценку фактической ценности конфигурации до и после изменения, при необходимости, применением разрешенных действий.

4. Требования гарантии, состоящие из уровня гарантии оценки.

В результате оценки должен быть сделан общий вывод, в котором указывается степень соответствия объекта оценки (АИС) функциональным требованиям и требованиям гарантированности. Измерение уровня гарантии основано на активном исследовании оцениваемой системы опытными оценщиками (экспертами) с увеличивающимся акцентом на возможностях, глубине и строгости методов оценки, а также на добавлении новых требований.

Анализ рассмотренных требований к безопасности и гарантии оценки требований, реализуемые на основе стандарта ССЕВ, позволяет грамотно провести не только оценку, но и уточнить или задать новые требования к безопасности информации в АИС.

Таким образом, *основное требование к системе защиты информации в АИС* можно сформулировать следующим образом: система защиты информации должна обеспечивать выполнение АИС своих основных функций и не снижать её технические возможности

6. Выводы. Высокие требования, предъявляемые к уровню информационной безопасности в АИС организаций, использованию её систем связи и передачи данных предопределяют необходимость проведения оценки эффективности систем защиты. Это сложная организационно-технологическая задача, которая требует системного подхода к её решению.

Оценка эффективности мер защиты информации должна проводиться с использованием технических и программных средств контроля на предмет соответствия установленным нормативным требованиям.

Трудности определения количественных и качественных оценок эффективности СЗИ, а следовательно, и объективного подтверждения их достоверности вызваны отсутствием единого методического подхода к оценке их эффективности.

Несовершенство существующего нормативно-методического обеспечения информационной безопасности в сложившихся информационных технологиях и подходах не позволяет развиваться и выходить на современный уровень безопасности.

Рассмотренные требования к безопасности и гарантии оценки требований, реализуемые на основе международного стандарта ССЕВ, позволяет грамотно провести не только оценку, но и уточнить или задать новые требования к безопасности информации в АИС.

Литература

1. Общее описание процедуры аттестации автоматизированных систем по требованиям информационной безопасности [Електронний ресурс] // – Режим доступу : http://kiev-security.org.ua/box/12/140.shtml.

2. Андрианов В. В. Оценка информационной безопасности бизнеса [Електронний ресурс] // – Режим доступу : http://www.cfin.ru/appraisal/business/special/infosec.shtml.

3. Маслова Н. А. Методы оценки эффективности систем защиты информационных систем / Н. А. Маслова // Искусственный интеллект. – 2008. – №4. – С.253-264.

4. Защита информации в автоматизированных системах обработки информации [Електронний ресурс] // – Режим доступу : http://www.xserver.ru/computer/raznoe/bezopasn/2/.

5. Общие критерии оценки безопасности информационной технологии [Електронний ресурс] // – Режим доступу : http://kiev-security.org.ua/box/12/106.shtml.

Дата надходження в редакцію: 29.07.2015 р. Рецензент: д.т.н., проф. О. О. Скопа