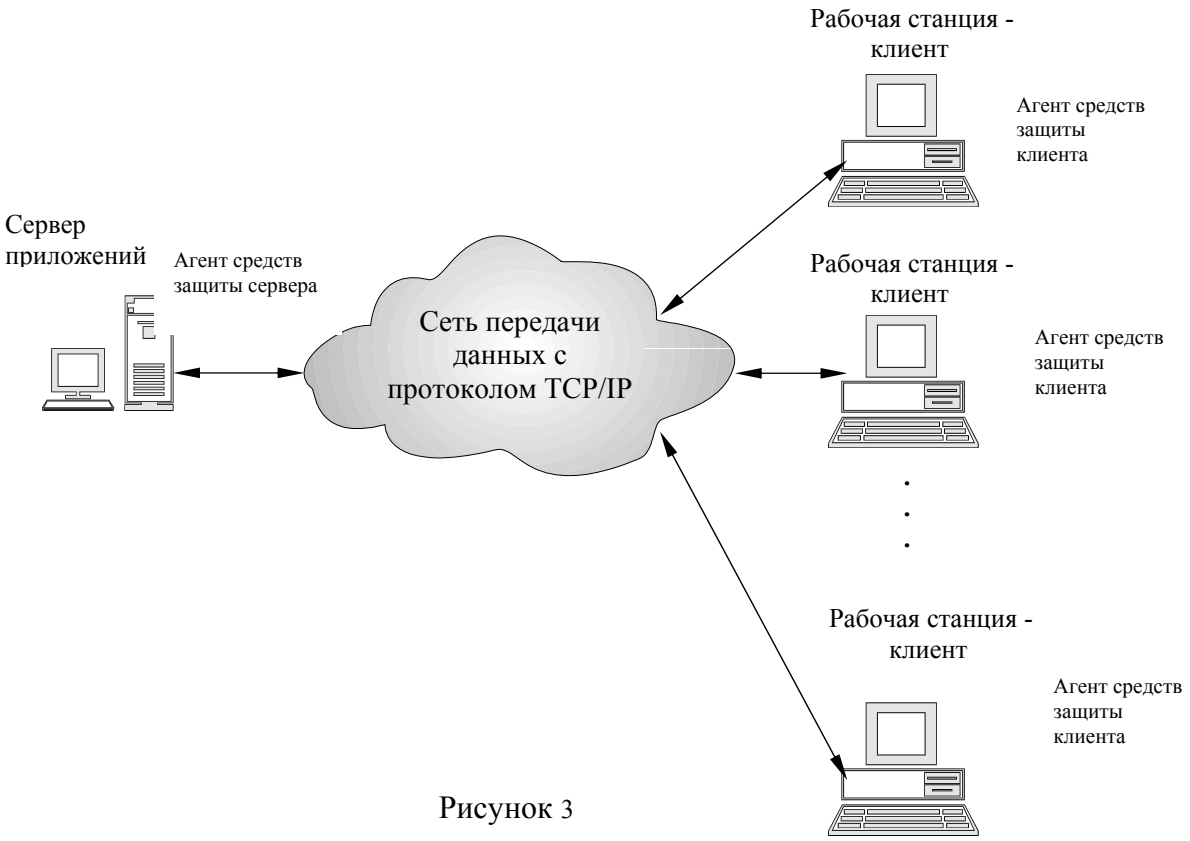

Рисунок 3

приложением. При этом приложение-сервер конфигурируется таким образом, чтобы допускать обработку запросов только от модуля - агента средств защиты сервера (только с сетевого адреса сервера приложений).

Литература: 1. Дениз Паппалардо. Виртуальная реальность? СЕТИ #05-06/99. 2. Роберт Ричардсон. Виртуальные частные сети: только между нами. Lan Magazine/Русское издание, (Март 1997, том 3, номер 2). 3. ITU Recommendation X. 509. The Directory: Authentication Framework (ISO/IEC 9594-8), 1993. 4. ISO 7498-2. Basic Reference Model – Part 2: Security Architecture. – February 1989.

УДК 681.3.067

К ПОСТРОЕНИЮ РАЦИОНАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ

Василий Бриль
Военный институт Национального технического университета Украины "КПІ"

Анотація: **Ефективний захист інформації не може бути забезпечений простим включенням у склад автоматизованих систем механізмів та пристроїв захисту – захистом інформації необхідно постійно керувати.**
Summary: **The effective protection of the information can not be ensured with prime actuation in a structure of the automized systems of gears and protective systems - the protect of the information is necessary permanently for controling.**
Ключові слова: **захист інформації, автоматизована система обробки даних.**

Известно, что обеспечение надежной защиты информации (ЗИ) не разовое мероприятие, а совокупность различных мероприятий, осуществляемых как во время разработки, так и эксплуатации автоматизированных систем обработки данных (АСОД).

На основе анализа развития концепции ЗИ нетрудно сделать вывод о том, что имеет место тенденция постоянного роста усилий, вкладываемых в защиту, совершенствование подходов к защите и самих механизмов защиты. Однако следует отметить и тот факт, что традиционная архитектура АСОД и технология автоматизированной обработки информации не обеспечивает всех условий, необходимых для надежной ЗИ [1, 2, 3].

В связи с этим необходимо сформулировать необходимые и достаточные требования к проектированию архитектуры и технологии функционирования АСОД, при выполнении которых возможна гарантированная надежная ЗИ.

Одним из основных подходов к проблеме ЗИ, является положение о том, что в современных и перспективных АСОД эффективная ЗИ не может быть обеспечена простым включением в состав автоматизированных систем некоторых механизмов и устройств защиты (рисунок 1) - ЗИ необходимо постоянно управлять [2].

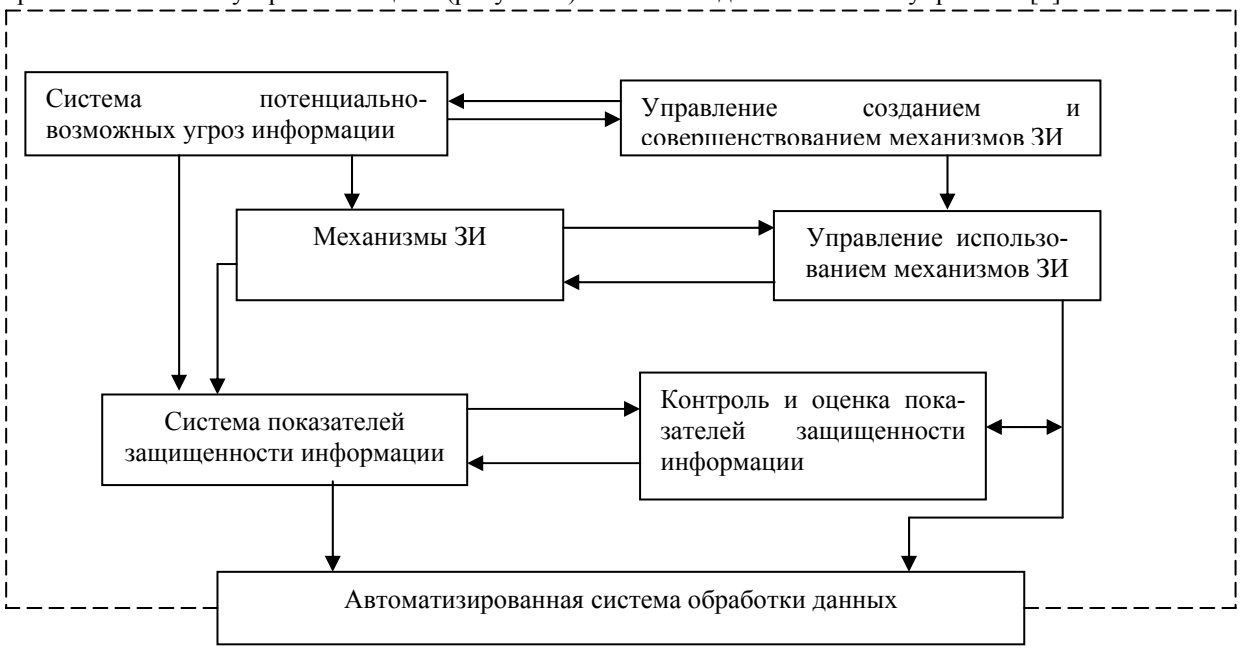

Рисунок 1 Обобщенная схема системы управления ЗИ

Как следует из рисунка 1, управление защитой информации представляет собою сложную совокупность взаимосвязанных процессов непрерывного создания, совершенствования и контроля над механизмами защиты, используемыми в АСОД. При этом важным является то обстоятельство, что система управления ЗИ представляет собой совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в АСОД с целью создания, поддержания и обеспечения условий, объективно необходимых для обеспечения надежной защиты информации требуемого уровня.

Под уровнем защищенности информации понимается отношение текущего значения показателя защищенности информации, действительно имеющего место, к требуемому значению соответствующего показателя. На основе оценки этого отношения принимается управленческое решение по использованию средств защиты.

В соответствии с основной посылкой о необходимости постоянного управления процессами ЗИ (рисунок 1) все элементы указанной последовательности разделены на две цепи: управления созданием механизмов защиты, управления и контроля над механизмами защиты.

При таком подходе очевидным является то обстоятельство, что названные процессы должны быть регулярными, постоянно управляемыми, причем управление должно осуществляться с целью достижения максимального уровня защиты, при соответствующих минимальных и сопоставимых с ценностью информации, затратах сил и средств.

В соответствии с требуемыми показателями защищенности должны быть определены оптимально достаточные наборы средств защиты (технических, программных, организационных и др.), обеспечивающих требуемый уровень защищенности. Обоснование таких наборов средств защиты является общей задачей механизмов управления средствами защиты.

Надежная ЗИ в АСОД может быть эффективной лишь в том случае, если она будет требуемой на всех объектах и всех элементах системы, которые могут быть подвергнуты угрозам со стороны возможных дестабилизирующих факторов при постоянном контроле показателей уровня защищенности системы [6].

Для определения уровня защищенности должен осуществляться соответствующий контроль, на основе которого определятся показатель уровня защищенности.

Представляется целесообразным привести наиболее существенные этапы контроля:

- контроль соответствия элементов системы, включающий проверку идентичности функционирующих элементов защиты, элементам заявленным;
- контроль состояния элементов системы, включающий проверку действительного их состояния в контролируемый момент времени;
- контроль правильности функционирования элементов системы, включающий проверку соответствия действительного функционирования элементов заявленным;
- контроль параметров внешней среды, включающий определение значений тех нерегулируемых параметров, которые оказывают (или могут оказывать) влияние на работоспособность системы защиты.

Основными характеристиками контроля (каждого из видов) являются: полнота контроля, количество охватываемых контролем элементов системы, время и периодичность проведения контроля, последовательность проводимых контрольных операций, режим проведения контроля, степень автоматизации контрольных операций, анализ и оценка хода выполнения контроля механизмов защиты с целью своевременного и правильного принятия решения.

Полнота контроля предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.

Задача контроля защищенности может быть сформулирована следующим образом. Осуществить мероприятия для решения следующих задач:

- сбор данных по всем параметрам, характеризующим защищенность информации;
- определение текущих значений всех требуемых параметров;
- определение текущих значений показателей защищенности;
- прогнозирование значений показателей защищенности;
- оценка показателей защищенности и принятие решения.

На основе данных контроля определяется показатель действительного уровня защищенности системы. Этот показатель сопоставляется с требуемым уровнем защиты и если рассогласование указанных показателей превышает допустимый порог, то система управления защитой должна отреагировать путем изменения набора используемых средств защиты или изменением показателя требуемого уровня защищенности.

Создание систем ЗИ может осуществляться в различных условиях, причем определяющее влияние на различие этих условий оказывают следующие подходы: первый - состояние автоматизированной системы, для которой разрабатывается система управления ЗИ, и второй - уровень затрат, которые могут быть допущены на создание системы управления ЗИ.

Что касается первого подхода, то, очевидно, можно выделить следующие возможные состояния системы: система обработки данных функционирует, имеется готовый проект системы или система еще только разрабатывается. Затраты на создание системы управления ЗИ могут быть заданы, в зависимости от уровня обеспечиваемой защиты или определяются в процессе проектирования.

Однако обоснование требований к ЗИ являются первоочередной и основополагающей задачей разработки систем защиты, поскольку результаты ее решения составляют исходную базу для решения всех последующих задач. В то же время, задача обоснований требований к построению системы управления ЗИ может решаться неформальными методами, поскольку формальные методы объективного обоснования требований отсутствуют и возможности их разработки для всех возможных случаев практического применения проблематичны. Поэтому задача обоснований может решаться исходя из разработки системы рекомендаций, исходя из современных возможностей и условий автоматизированной обработки информации.

С целью целенаправленного выбора требований, каждому элементу АСОД, имеющему самостоятельное территориальное размещение, должна быть определена категория по требуемому уровню защищенности при соблюдении всех специальных требований, которые обусловлены категорией системы обработки данных. Этот вывод подтверждаются тем, что защита информации есть сложный процесс в том смысле, что защищать информацию надо не только непосредственно в структурных элементах информационной системы обработки данных, но также и в помещениях, где установлены средства обработки, и на территории, где расположены соответствующие помещения. Очевидным является и то обстоятельство, что защита информации может считаться надежной, по заданному уровню защиты, если она осуществляется во всех контролируемых зонах [4].

Учитывая тот факт, что управление защитой информации является частным случаем управления в системах организационно-технологического типа, то это обстоятельство облегчает проектирование систем защиты,

поскольку для этого достаточно трансформировать общие положения концепции управления в системах указанного типа на проблемы управления защитой информации.

Исходя из вышеизложенного, представляется, что такой подход к построению возможной системы управления защитой информации, обеспечивает достаточно четкие ориентиры, как для разработки систем защиты в информационных системах обработки данных, так и для их выбора в процессе решения вопросов защиты информации.

Литература: 1. Бриль В.М. Криптографические методы защиты информации. - К.: МОУ, 1996. - 233 с. 2. Бриль В.М., Бриль Ю.В. Захист інформації в сучасних та перспективних системах обробки даних. - К.: КМУЦА, 1998. - 101 с. 3. Бриль В.М. Сучасні методи і засоби криптографічного перетворення інформації з метою її захисту. - К.: НТУУ «КПІ», 1999. - 83 с. 4. Бриль В.М., Нестеренко С.Д., Шаталюк В.В. Оценка показателей уязвимости информации при несанкционированном доступе. - К.: Нсб. ЗИ, 2000. - 156 с. 5. Хоффман Л.Дж. Современные методы защиты информации. - М.:» Сов. радио», 1980. - 264 с.

УДК 621.391.7:336.71(075.8)

ВПЛИВ ВИПАДКОВИХ ФАКТОРІВ НА БЕЗПЕКУ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ БАНКА

Анатолій Бєгун, Володимир Жлуктенко, Максим Плахтій
Київський Національний економічний університет

Анотація: **В цій статті розглянуто вплив випадкових факторів на безпеку технологічного процесу банка**
Summary: **In this article was examined the influence of accidental factors on safety of technological process of bank**
Ключові слова: **безпека, банк, технологічний процес, випадкові фактори**

I Вступ

Інформаційна незалежність України ставить ряд проблем забезпечення безпеки інформації в різноманітних напрямках діяльності держави: політика, економіка, військова сфера, тощо.

Особливе місце в цих проблемах займає задача захисту економічної інформації, яка набуває всебічного, масштабного характеру та державної ваги. Одним з зфакторів забезпечення безпеки економічної інформації є захист фінансово-банківської системи.

Розглянемо, як приклад, загальний технологічний процес обліку операцій за пластиковими картками банку. Цей процес має деяку сукупність об'єктів, які зв'язані між собою інформаційними подіями. Кількість об'єктів і зв'язків між ними є величиною обмеженою з випадковим впливом відповідних факторів під час проходження процесу. Ці фактори призводять до порушення стаціонарного режиму функціонування технологічного процесу і складають умови для несанкціонованого доступу до окремих об'єктів, витоку та знищення інформації.

Загальна схема технологічного процесу наведена на рисунку 1.

Рисунок 1