

В настоящем сборнике и представлен ряд результатов исследований и разработок специалистов ХТУРЭ и АТ «Институт информационных технологий» в указанных направлениях. Издание сборника такой направленности позволит довести до специалистов и интересующихся проблемами защиты информации ряд новых результатов и достижений, развернуть дискуссии.

Конечно же, статьи отражают, прежде всего, мнения и взгляды авторов по обсуждаемым проблемам, в то же время статьи к опубликованию кафедрой «Безопасность информационных технологий» и ХТУРЭ. В целом считаем, что публикация статей в тематическом сборнике позволит ускорить процессы освоения и использования известных методов и средств криптографической защиты информации, обоснования требований к разработке перспективных. С учетом этого и производится отбор статей.

С уважением и благодарностью к специалистам и читателям, которые интересуются проблемами информационной безопасности.

Ректор ХТУРЭ, профессор



М.Ф. Бондаренко

Заведующий кафедрой БИТ, профессор



И.Д. Горбенко

ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ СОЗДАНИЯ И РАЗВИТИЯ ПЕРСПЕКТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06:519.248.681

*М. Ф. БОНДАРЕНКО, д-р техн. наук, С. П. ЧЕРНЫХ, И. Д. ГОРБЕНКО, д-р техн. наук,
А. А. ЗАМУЛА, канд. техн. наук, А. А. ТКАЧ*

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ КОНЦЕПЦИИ И ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Введение

В постоянно расширяющейся области использования средств вычислительной техники и передачи данных появляются все новые и новые проблемы сохранения конфиденциальности, целостности, наблюдаемости и доступности информации, ограждения её от посягательств злоумышленников. Наиболее надежную защиту информации в автоматизированных системах и сетях (далее – Системах) различных классов можно обеспечить только с помощью системного подхода. Он предполагает, что решение задачи должно достигаться за счет использования совокупности организационных и организационно-технических мер и мероприятий, а также криптографических систем и средств. Системный подход ориентирован на создание комплексной системы защиты информации (КСЗИ) в Системе [1,2].

Процесс создания КСЗИ включает три основных этапа [3]:

- предварительный;
- проектирования и разработки КСЗИ;
- проведение испытаний и сдача в эксплуатацию КСЗИ.

На предварительном этапе выполняются следующие основные работы:

- 1) классификация и описание ресурсов Системы (вычислительной системы, способов связи и коммуникаций, информации, ее категорий, вида представления, мест хранения, технологии обработки и тому подобного, обслуживающего персонала и пользователей, территории и помещений и т.п.);
- 2) разработка информационной модели для существующей Системы, то есть описание (формальное или неформальное) информационных потоков Системы, интерфейсов между пользователем и Системой и т. п.;
- 3) определение перечня угроз и возможных каналов утечки информации;
- 4) экспертная оценка ожидаемых потерь в случае осуществления угроз; определение услуг безопасности, которые должны предоставляться пользователям;
- 5) обоснование необходимости проведения спецпроверок и специсследований средств вычислительной техники (СВТ) и других технических средств, а также специального оснащения помещений;
- 6) определение требований к организационным, физическим и другим мероприятиям защиты, которые реализуются в дополнение к комплексу программно-технических способов защиты;
- 7) определение требований к метрологическому обеспечению работ;
- 8) определение перечня макетов, которые разрабатываются, и технологических стендов;
- 9) оценка стоимости и эффективности избранных способов;
- 10) принятие окончательного решения о составе КСЗИ Системы.

По результатам выполненных на предварительном этапе работ формируются документы: «Политика безопасности информации Системы» и «Концепция безопасности информации Системы». Кроме того, разрабатывается ТЗ на создание КСЗИ Системы и совокупность документов, в соответствии с которыми осуществляется организация защиты информации на всех этапах жизненного цикла Системы — «План защиты информации в Системе».

Следует отметить, что разработка политики и концепции безопасности Системы, должна предшествовать разработке ТЗ на создание КСЗИ Системы и Плана защиты информации в Системе.

1. Разработка Политики безопасности информации в АС

Под политикой безопасности информации в Системе (далее – политика безопасности Системы) будем понимать набор законов, нормативных документов, требований, правил, ограничений, инструкций, рекомендаций и т.п., которые регламентируют порядок обработки информации и направлены

на защиту информации от определенных угроз [3, 4]. Политика безопасности разрабатывается для отдельного компонента Системы, услуги защиты и Системы в целом. Политика безопасности информации в Системе является частью общей политики безопасности организации и должна наследовать основные ее принципы и положения.

Содержание политики безопасности Системы определяется технологией обработки информации, моделями нарушителей и угроз, особенностями вычислительной системы (ВС), физической среды и прочими факторами. Вследствие этого, если в какой-либо Системе реализуются различные технологии обработки информации, то и политика безопасности в такой Системе будет состоять из нескольких существенно отличных частей, каждая из которых будет отвечать конкретной технологии обработки информации. Как составные части общей политики безопасности Системы могут разрабатываться политики обеспечения конфиденциальности, целостности, наблюдаемости и доступности обрабатываемой информации, а также правила разграничения доступа (ПРД), которые регламентируют правила доступа пользователей и процессов к ресурсам Системы.

Политика безопасности должна предусматривать комплексное использование правовых и нравственно-этических норм, организационных (административных) мер, физических, технических (аппаратных и программных) способов и средств защиты информации, а также определять правила и порядок их применения в Системе. Политика безопасности должна базироваться на принципах системности, комплексности, непрерывности защиты, достаточности механизмов и мероприятий защиты и их адекватности угрозам, гибкости управления системой защиты, простоты и удобства ее использования, открытости алгоритмов и механизмов защиты, если другое не предусмотрено в отдельности.

Политика безопасности Системы должна доказательно давать гарантии того, что:

- в Системе (в каждой отдельной составной части, в каждой функциональной задаче и т. п.) обеспечивается адекватность уровня защиты информации уровню ее критичности;
- реализация мероприятий защиты информации является рентабельной;
- в любой среде функционирования Системы обеспечивается оцениваемость и проверяемость защищенности информации;
- обеспечивается персонификация положений политики безопасности (относительно субъектов Системы), отчетность (регистрация, аудит) для всех критичных с точки зрения безопасности ресурсов, к которым осуществляется доступ;
- персонал и пользователи обеспечены достаточно полным комплектом документации относительно порядка обеспечения защиты информации;
- все критичные с точки зрения безопасности информации технологии (функции) Системы имеют соответствующие планы обеспечения непрерывной работы и ее возобновления в случае возникновения непредвиденных ситуаций.

Методология разработки политики безопасности включает в себя следующие работы:

- разработка концепции безопасности информации в Системе;
- анализ рисков;
- определение требований к методам и средствам защиты;
- выбор основных решений по обеспечению безопасности информации;
- организация выполнения восстановительных работ и обеспечение непрерывного функционирования Системы;
- документальное оформление политики безопасности.

В общем случае документ «Политика безопасности Системы» должен включать в себя описание [3, 4]:

- 1) объектов (элементов ресурсов) Системы;
- 2) основных угроз информации;
- 3) требований по защите от угроз;
- 4) принципов управления доступом пользователей к информации;
- 5) правил разграничения информационных потоков;
- 6) правил маркирования носителей информации;
- 7) основных атрибутов доступа пользователей, процессов и пассивных объектов;
- 8) правил разграничения доступа пользователей и процессов к пассивным объектам;

9) правил администрирования КСЗИ и регистрации действий пользователей.

В разделе «Описание объектов (элементов ресурсов) Системы» на основе инвентаризации (идентификации) всех компонентов Системы, участвующих в технологическом процессе обработки информации, приводится описание критичных с точки зрения безопасности активных и пассивных компонентов Системы.

Инвентаризации (идентификации) подлежат:

- организационно-топологическая структура Системы, для которой создается КСЗИ;
- состав и назначение функциональных подсистем Системы;
- состав служб и протоколов, реализующих информационный обмен между элементами (компонентами) Системы;
- объекты защиты (виды и категории обрабатываемой информации, аппаратно-программные и информационные ресурсы на соответствующих уровнях иерархической структуры Системы);
- персонал и пользователи Системы.

При описании компонентов Системы рекомендуется составить структурную схему информационных потоков между основными компонентами Системы, а также описать (формально или неформально) технологию обработки информации. При выборе и анализе объектов Системы важным моментом является степень детализации рассматриваемых объектов. Так, для Системы 1-го класса (отдельная ПЭВМ) допустимо рассматривать всю инфраструктуру, тогда как для Системы 3-го класса (глобальная сеть) всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В этом случае рекомендуется сосредоточиться на описании наиболее важных компонентов Системы.

В разделе «Описание основных угроз информации» на основе анализа рисков приводится перечень и классификация возможных видов угроз безопасности информации в Системе. Под угрозой безопасности понимаются какие-либо обстоятельства или действия, которые могут быть причиной нарушения политики безопасности информации и /или нанесения ущерба Системе. Ущерб заключается в нарушении качества информации пользователей (в семантическом и прагматическом смысле) путем её уничтожения, изменения или несанкционированного получения, либо в уничтожении, изменении или несанкционированном использовании ресурсов Системы. В зависимости от класса Системы анализ угроз необходимо осуществлять на уровне отдельных аппаратных, аппаратно-программных и программных средств, отдельной локальной вычислительной сети, глобальной сети. Анализ рисков предусматривает разработку модели угроз для информации и модели нарушителя, установление соответствия модели угроз и объектов защиты, оценку возможности реализации угрозы (оценка риска), количественную либо качественную оценку величины возможного ущерба вследствие реализации угроз конфиденциальности, целостности, наблюдаемости или доступности информации либо потери управляемости Системы. Для разработки модели угроз необходимо сформировать перечень основных угроз и описать возможные способы их осуществления на основе анализа объектов Системы, характеристик вычислительной системы (ВС), физической среды, персонала, особенностей функционирования Системы.

В разделе «Требования по защите от угроз» приводятся основные задачи и цели защиты информации, объекты защиты, выбранный вариант построения КСЗИ Системы. С учетом класса Системы [5, 6] для каждого компонента и /или Системы в целом перечисляются функциональные услуги безопасности и требования к уровням реализации каждой из них, уровень гарантий реализации услуг. Для каждого компонента и /или Системы в целом определяются общие подходы и требования по защите информации от утечки техническими каналами. На следующем шаге определяются механизмы безопасности, которые реализуют функциональные услуги безопасности, осуществляется выбор технических средств защиты информации от утечки техническими каналами. При необходимости определяются компоненты Системы (например, отдельная ЛВС, специализированный АРМ, Internet-узел и т. п.), для которых целесообразно разрабатывать свои собственные политики безопасности, отличные от общей политики безопасности Системы. Исходными данными для разработки требований по защите от угроз являются задачи и функции Системы, результаты анализа среды функционирования Системы, модель угроз, модель нарушителей, результаты анализа рисков.

В разделе «Описание принципов управления доступом пользователей к информации» приводятся выбранный метод управления доступом (доверительное и /или административное управление), требования к обеспечению непрерывности защиты, к набору атрибутов доступа и правилам их использования (присвоение, применение, изменение, отмена), к регистрации действий пользователей

при использовании ресурсов Системы, а также других событий, влияющих на соблюдение реализованной в Системе политики безопасности.

В разделе «Описание правил разграничения информационных потоков» приводится перечень информационных потоков, циркулирующих между компонентами Системы. В зависимости от класса Системы структурная схема информационных потоков между основными компонентами Системы может включать:

- внутренние потоки обмена между активными и пассивными объектами внутри одной ПЭВМ;
- локальные потоки обмена между рабочими станциями и серверами внутри одной ЛВС (домена);
- межсетевые потоки обмена между ЛВС (доменами), входящими в состав одной Системы;
- потоки обмена информацией с удаленными взаимодействующими объектами, не входящими в состав Системы.

Правила разграничения информационных потоков формулируются на основе анализа области (границы) существования, направленности (входные или выходные), источников и приемников, функционального назначения потоков, требований по обеспечению конфиденциальности, целостности, наблюдаемости и доступности. Правила должны определять, где и на каких уровнях взаимодействия систем должно осуществляться разграничение информационных потоков и с использованием каких атрибутов и механизмов (идентификаторов безопасности, сетевых портов, ключей аутентификации, ключей направлений и сетевых ключей шифрования и т. п.). Правила должны также определять условия и ограничения по инициированию и завершению процессов информационного обмена, например, в виде ассоциации безопасности [7].

В разделе «Описание правил маркирования носителей информации» приводятся правила, регламентирующие порядок учета, хранения, копирования, использования и уничтожения носителей информации. Правила формулируются на основе изучения форм существования критичной информации на всех этапах жизненного цикла Системы, среды функционирования Системы, модели угроз для информации и модели нарушителей, результатов анализа рисков, требований по обеспечению конфиденциальности, целостности наблюдаемости и доступности информации

В разделе «Описание основных атрибутов доступа пользователей, процессов и пассивных объектов» приводятся состав атрибутов доступа (идентификационные имена, индивидуальные и групповые идентификаторы безопасности, пароли, метки и /или маркеры доступа, списки контроля доступа и т. п.), требования к характеристикам атрибутов доступа (принадлежность, уникальность, размерность, сроки действия и т. п.) и правила работы с ними (присвоение, использование, модификация, отмена)

В разделе «Описание правил разграничения доступа пользователей и процессов к пассивным объектам» содержится набор правил определяющих состав лиц, которым разрешен доступ к ресурсам Системы, порядок правильного использования ресурсов Системы, статус, права и привилегии администратора безопасности Системы, статус, права и привилегии пользователей Системы.

В разделе «Описание правил администрирования КСЗИ и регистрации действий пользователей» приводится порядок администрирования учетных записей пользователей, профилей пользователей, групп пользователей, общих ресурсов и аудита.

2. Разработка концепции безопасности информации в АС

Концепция безопасности информации в Системе представляет собой совокупность взглядов, общих принципов и определяет основные положения и направления обеспечения безопасности информации в Системе, а также целенаправленной организации всех работ по созданию КСЗИ. Разработка документа «Концепция безопасности информации Системы» осуществляется на основе концепции построения Системы.

Методология разработки концепции безопасности включает в себя следующие работы:

- 1) анализ правовых и договорных основ создания Системы;
- 2) изучение архитектуры создаваемой Системы и технологических процессов обработки информации с целью определения активных и пассивных компонентов, влияющих на безопасность информации;
- 3) определение совокупности угроз и степени уязвимости ресурсов Системы (включая передаваемую, обрабатываемую и хранимую информацию);
- 4) определение требуемого уровня обеспечения безопасности информации;

5) определение множества средств, методов и мероприятий защиты.

По результатам выполнения работ должны быть сформулированы общие положения безопасности, которые определяют:

— цель и приоритеты, которых необходимо придерживаться в Системе во время обеспечения безопасности информации;

— общие направления деятельности, необходимые для достижения этой цели;

— аспекты деятельности в области безопасности информации, которые должны учитываться на уровне организации в целом;

— ответственность должностных лиц и других субъектов взаимоотношений в Системе, их права и обязанности относительно реализации задач безопасности информации.

В общем случае документ «Концепция ...» должен включать следующие разделы:

1) область применения;

2) общие положения;

3) основные понятия;

4) цели обеспечения безопасности информации в Системе;

5) цель создания КСЗИ в Системе;

6) угрозы, объекты и задачи защиты информации в Системе;

7) концептуальные принципы и основные положения по обеспечению безопасности информации в Системе;

8) основные направления решения проблем обеспечения безопасности информации в Системе;

9) требования к подсистеме криптографической защиты информации КСЗИ Системы;

10) требования к архитектуре КСЗИ Системы;

11) этапы развития КСЗИ Системы.

В зависимости от конкретного класса Системы [6], архитектуры и условий функционирования Системы, исходных требований собственника и возможных пользователей Системы по обеспечению безопасности информации (в т. ч. по криптографической защите), допускается, в случае необходимости, объединять отдельные разделы в один, вводить новые разделы (подразделы) либо исключать неактуальные разделы.

В разделе «Область применения» излагается назначение и предметная область документа.

В разделе «Общие положения» излагаются результаты системного анализа архитектуры построения и состава пользователей Системы, исходных требований собственника и возможных пользователей Системы по обеспечению безопасности информации (в т. ч. по криптографической защите), состава нормативно-правовой базы создания концепции безопасности информации Системы. В случае отсутствия исходных данных и требований возможных пользователей Системы по обеспечению безопасности информации системный анализ возможной архитектуры построения Системы рекомендуется проводить, исходя из следующих предпосылок:

1) пользователи и информационные процессы, являющиеся получателями и источниками информации с ограниченным доступом, осуществляют взаимодействие посредством службы 7 (прикладного) уровня Системы;

2) по отношению к анализируемой Системе сторонние пользователи не обладают правами владения, эксплуатации и распоряжения её элементами;

3) пользователи Системы (в т. ч. сторонние пользователи) в соответствии с законами Украины «Об информации» и «О защите информации в автоматизированных системах» и др. могут предъявлять требования по обеспечению их права собственности на информацию;

4) система криптографической защиты информации каждого пользователя (группы пользователей) относительно систем других пользователей (групп пользователей) в сетях Системы должна быть выделенными и включать только объекты данного пользователя (группы пользователей);

5) информация, зашифрованная пользователем, должна передаваться по сетям Системы без её расшифрования на ретрансляционных узлах (станциях, центрах);

6) эксплуатация систем защиты информации (в т. ч. криптографической защиты информации) должна осуществляться только соответствующими службами пользователей и /или владельца (оператора) Системы;

7) использование зарубежных не сертифицированных в Украине аппаратных, аппаратно-программных и программных средств защиты информации неприемлемо;

— связанные участием в обеспечении качества информации с другими функциональными подсистемами как в каждой составной части, так и Системы в целом;

6) КСЗИ Системы должна представлять собой совокупность правовых (законодательных), организационных и технических мер, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба интересам владельца (оператора) Системы, а также её пользователям (юридическим и физическим лицам, являющимися собственниками передаваемой информации);

7) политику безопасности информации в Системе и её составных частях определяют владельцы информации (пользователи Системы) в порядке, установленном соответствующими органами государственного управления;

8) объектами защиты в Системе и её составных частях являются:

- информация пользователей и информационные процессы в системах управления (информационных системах) пользователей;
- информация о Системе и её элементах;
- управляющие процессы в Системе, включая служебную управляющую информацию;
- ресурсы Системы и ее составных частей (средства связи и управления, информационно-программное обеспечение, линии связи и т. п.);

9) циркулирующая в Системе информация пользователей и служебная информация по обеспечению функционирования системы (подсистемы, элемента), как объекты защиты, имеют различный статус :

- информация с ограниченным доступом (ИсОД), включающая сведения, составляющие государственную тайну, и конфиденциальные сведения;
- открытая информация;

10) КСЗИ Системы должна обеспечивать защиту от следующих видов угроз: (перечень угроз определяется моделью угроз и моделью нарушителя, разработанных для конкретной Системы);

11) по проявлению и положению источников возникновения угроз относительно составных частей Системы и её элементов угрозы группируются на классы. В свою очередь классы угроз включают совокупности угроз, сгруппированные по каналам реализации: (классы и группы угроз определяются для конкретной Системы);

12) принимая во внимание широкий круг пользователей, возможность размещения оборудования Системы на территориях, неконтролируемых владельцем Системы, выход на зарубежные системы телекоммуникаций, широкое использование зарубежной техники и технологий потенциально возможные угрозы безопасности информации пользователей и безопасности Системы могут проявляться в каждой составной части и Системе в целом на уровне:

- отдельных аппаратно – программных устройств (ПЭВМ, модем, операционная система, база данных, телефонный/ телеграфный аппарат и т.п.);
- отдельных локальных сетей и подсистем (комплекс, аппаратная, центр и т.п.);
- отдельной сети и Системы в целом (при работе по наземным и спутниковым магистральным, зонным и внутризональным каналам и трактам передачи);

13) исходя из перечня возможных угроз, КСЗИ Системы должна обеспечивать:

- целостность пользовательской и служебной информации на всех этапах её обращения при любых угрозах;
- подтверждение подлинности пользовательской и служебной информации на всех этапах её обращения при любых угрозах;
- юридическую защиту взаимодействующих сторон (пользователей, станций) на основе модели взаимного недоверия между ними;
- информационную скрытность информации с ограниченным доступом, циркулирующей в Системе;
- защиту от несанкционированного доступа к защищаемой информации и ресурсам Системы;

- юридическую ответственность взаимодействующих сторон за сформированные, переданные, принятые и обработанные сообщения (данные);

- организационно – технические и юридические меры защиты информации с ограниченным доступом от утечки.

14) реализация функций и задач КСЗИ Системы должна обеспечиваться комплексным использованием методов и средств криптографической и технической защиты информации;

15) функциональная структура КСЗИ составных частей и Системы в целом должна включать следующие функции безопасности: (перечень функциональных услуг определяется для конкретной Системы по результатам анализа рисков);

16) реализация функций КСЗИ Системы должна обеспечиваться внедрением следующих средств (механизмов) защиты: (состав механизмов защиты определяется для конкретной Системы по результатам формирования функциональной структуры КСЗИ и модели угроз);

17) комплекс правовых (законодательных), организационных (административных), технических и физических мероприятий и средств, реализующий функции и задачи КСЗИ Системы, должен обеспечивать:

- предупреждение условий, порождающих угрозы;
- предупреждение проявления угроз;
- обнаружение проявления угроз;
- предупреждение воздействия угроз на объекты защиты;
- обнаружение воздействия угроз на объекты защиты;
- локализацию воздействия угроз на объекты защиты;
- ликвидацию последствий воздействия угроз на объекты защиты;

18) обеспечение безопасности информации в составных частях и Системе в целом должно осуществляться комплексом правовых (законодательных), организационных (административных), морально-этических, физических и технических мер, реализующих следующие методы обеспечения безопасности:

- препятствия (физическое преграждение пути);
- управление доступом (регулирование использования всех ресурсов Системы);
- маскировка (скрытие содержания информации криптографическими методами);
- регламентация (создание условий, минимизирующих возможность несанкционированного доступа к информации);
- принуждение (соблюдение установленных правил использования ресурсов системы, в т.ч. информации под угрозой наступления ответственности);
- побуждение (выполнение установленных правил использования ресурсов системы, в т.ч. информации за счет соблюдения сложившихся моральных и этических норм);

19) обеспечение безопасности информации в Системе может быть эффективным только в том случае, если оно будет представлять собою непрерывный и целенаправленный процесс, регулярно осуществляемый на всех этапах жизненного цикла. Поэтому КСЗИ Системы помимо функций, задач и средств собственно обеспечения защиты информации должна включать функции, задачи и средства управления в качестве одного из основных компонент;

20) КСЗИ Системы и её составных частей должна реализовываться на принципах:

- системности (учёт с позиций системного подхода всех взаимосвязанных и изменяющихся во времени элементов, условий, обстоятельств и факторов, существенно значимых для обеспечения безопасности информации в Системе);
- комплексности (согласованное использование различных средств и методов защиты при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз);
- непрерывности (обеспечение защиты на всех этапах жизненного цикла Системы и её составных частей);

- адекватности требованиям (построение КСЗИ Системы должно осуществляться в соответствии с требованиями политики безопасности);
- адаптируемости (способность к целенаправленному приспособлению при изменении архитектуры или условий функционирования Системы, в т.ч. видов и классов угроз);
- функциональной самостоятельности (при осуществлении функций защиты не зависеть от других функциональных подсистем Системы);
- удобства использования (не должна создавать дополнительных неудобств для пользователей и персонала Системы);
- минимизации предоставляемых прав (каждому пользователю и каждому лицу из состава персонала Системы должны предоставляться только те полномочия на доступ к услугам и ресурсам составных частей и Системы в целом (в т.ч. к информации), которые действительно необходимы для выполнения своих функций);
- полноты контроля (должны контролироваться все каналы уязвимости информации пользователей и ресурсов составных частей и Системы в целом);
- активности и своевременности реагирования (должны быть своевременные реакции на любые атаки);
- управляемости процессами обеспечения безопасности информации в Системе;
- экономичности (расходы на КСЗИ Системы должны быть минимальными);

21) помимо этого КСЗИ Системы, как функциональные подсистемы каждой составной части и Системы в целом, должны отвечать требованиям:

- функциональным (обеспечение реализации требуемой совокупности функций и задач защиты, удовлетворение всем требованиям защиты);
- организационным (структурированность всех компонент, простота эксплуатации);
- техническим (оптимальность архитектуры, комплексное использование средств);
- экономическим (максимальное использование серийных средств, минимизация затрат на систему);
- эргономическим (минимизация помех пользователям, удобство для персонала системы связи);
- открытости (способность к развитию без нарушения функционирования);

22) при работе пользователей по постоянным виртуальным каналам или коммутируемым виртуальным соединениям через ретрансляционные узлы (центры, станции), не принадлежащие пользователям:

- зашифрование информации пользователей целесообразно осуществлять на 7 уровне с использованием всех служб зашифрование [8]. Осуществлять зашифрование информации пользователей с использованием служб зашифрование соединения на 1 – 4 уровнях, зашифрование без соединения на 2 – 4 уровнях, засекречивания потока данных на 1 уровне нецелесообразно, т. к. для нормального функционирования служб данных уровней требуется расшифрование данных пользователей на ретрансляционных узлах (станциях, центрах) общего пользования в процессе передачи;
- аутентификацию пользователей целесообразно осуществлять на 7 уровне с использованием служб аутентификации одноуровневых объектов или источников данных [8]. Осуществлять аутентификацию пользователей с использованием служб аутентификации одноуровневых объектов или источников данных на 3 и 4 уровнях (с применением механизмов симметричного шифрования, формирования цифровой подписи и обеспечения аутентификации) нецелесообразно, т. к. для нормального функционирования служб данных уровней в процессе установления соединения (или периодически в течение фазы передачи данных) в общем случае требуется рассекречивание аутентифицирующей пользователей информации на ретрансляционных узлах (станциях, центрах) общего пользования;
- реализация службы контроля доступа к ресурсам Системы на 3, 4 и 7 уровнях [8] аналогична вышеизложенному, т. к. содержит процедуры аутентификации;

23) при работе пользователя по выделенным либо по коммутируемым каналам связи, соединяющим узлы (станции) данного пользователя в качестве ретрансляционных:

- зашифрование информации пользователя с использованием служб засекречивания соединения на 1 – 4 уровнях, зашифрование потока данных на 1 и 3 уровнях, засекречивания без соединения и зашифрование выборочных полей на 2 – 4 уровнях возможна, т. к. объекты будут контролироваться его соответствующей службой;

- аутентификация пользователя с использованием служб аутентификации одноуровневых объектов или источников данных на 3 и 4 уровнях (с применением механизмов симметричного шифрования, формирования цифровой подписи и обеспечения аутентификации) возможна, т. к. объекты будут контролироваться соответствующей службой пользователя;

- реализация службы контроля доступа к ресурсам Системы на 3, 4 и 7 уровнях аналогична вышеизложенному т. к. содержит процедуры аутентификации;

24) для доставки пакетов сообщения блоки данных пользователей, в т. ч. содержащиеся в служебной части сообщения истинные адреса (нумерация, наименования) источника и получателя, должны быть оформлены в форме блоков данных (N) – протокола и засекречены. Для организации информационного обмена в телеинформационной системе блоки данных (N) – протокола пользователей должны представляться в форме блока данных (N) – службы и передаваться в форме блока данных (N) – интерфейса с присвоением пользователям в управляющей информации (N) – протокола (интерфейса) сетевых (условных) адресов;

25) реализация служб целостности (соединения с восстановлением, соединения без восстановления, выборочных полей соединения, без соединения, выборочных полей без соединения) на 3, 4 и 7 уровнях протокола информационного обмена передающего и принимающего объектов пользователя возможна как при работе пользователя по постоянным виртуальным каналам или коммутируемым виртуальным соединениям через не принадлежащие пользователю ретрансляционные узлы (центры, станции), так и при работе по выделенным либо коммутируемым каналам связи, соединяющим узлы (станции) данного пользователя в качестве ретрансляционных;

26) реализация служб защиты от отказов с подтверждением источника и защиты от отказов с подтверждением доставки на 7 уровне протокола информационного обмена передающего и принимающего объектов пользователя возможна как при работе пользователя по постоянным виртуальным каналам или коммутируемым виртуальным соединениям через не принадлежащие пользователю ретрансляционные узлы (центры, станции), так и при работе по выделенным либо коммутируемым каналам связи, соединяющим узлы (станции) данного пользователя в качестве ретрансляционных;

27) если безопасность информации обеспечивается пользователем собственными средствами на уровне приложения (информационного процесса), то допускается работа пользователя по постоянным виртуальным каналам или коммутируемым виртуальным соединениям через ретрансляционные узлы (станции), не принадлежащие пользователю, либо по выделенным или по коммутируемым каналам связи, через ретрансляционные узлы (станции) пользователя, с использованием всех служб засекречивания на 1 – 4 и 7 уровнях, служб аутентификации на 3, 4 и 7 уровнях и служб контроля доступа к ресурсам Системы на 3, 4 и 7 уровнях;

28) так как КСЗИ являются функциональными подсистемами как в каждой составной части, так и Системы в целом, их архитектура должна быть аналогична архитектуре соответствующей составной части и архитектуре Системы в целом.

В разделе «Основные направления решения проблем обеспечения безопасности информации в Системе» излагается перечень основных направлений построения КСЗИ Системы, реализация которых позволит решить поставленные задачи защиты информации в Системе, например:

1) базирование КСЗИ Системы преимущественно на национальных средствах защиты. В переходный период допускается использование зарубежных средств при условии обязательной сертификации и аттестации их национальными службами;

2) внедрение систем многоуровневой защиты, которые включают оперативные пункты (центры) управления (администраторов безопасности), службы и механизмы безопасности в соответствии с рекомендациями нормативных документов ДСТСЗИ СБУ, стандартов ISO 7498-2, ISO 15408;

3) использование доменов (модель «несколько мастер – доменов» или модель «домены с целиком доверительными отношениями») для организации локальных и распределенных сетей Системы;

4) применение систем защиты типа FireWall (фильтрующие маршрутизаторы, программные фильтры, шлюзы приложений) в вариантах организации схем защиты «демилитаризованная зона»

(demilitarized zone) или «бастиона серверов» (bastion servers) для защиты информационных ресурсов Системы в доменах локальных сетей от возможных угроз со стороны Internet или удаленных пользователей;

5) широкое применение криптографических аппаратных, аппаратно – программных и программных средств для защиты информации от несанкционированного доступа, нарушения целостности, модификации и хищений, включая:

- комплексное использование канального и межконцевого (абонентского) методов криптографической защиты;
- переход от центров распределения ключей к центрам управления ключами с использованием многоуровневой иерархии ключей;
- создание электронных систем генерации, учета и распределения ключей (включая разработку состоятельных протоколов передачи и подтверждения подлинности ключей, источника и получателя);
- использование методов цифровой подписи на базе несимметричных криптосистем;
- преимущественно аппаратная реализация криптоалгоритмов в виде модулей (блоков), которые встраиваются в аппаратуру управления и связи (коммутаторы, модемы, телефонные аппараты, ПЭВМ, радиостанции и т.п.);
- уменьшение энергопотребления и массогабаритных характеристик за счет внедрения микропроцессорной техники и современных технологий;
- повышение скорости шифрования до 10 – 100 Мбит/с;

6) внедрение многоуровневых систем паролирования для аутентификации и контроля полномочий объектов (пользователей, терминалов и т.п.), в т.ч. с применением интеллектуальных карточек различных типов (в т.ч. с криптографическими ключами);

7) широкое использование базового программного обеспечения (ОС, СУБД) с встроенными сертифицированными системами защиты информации;

8) унификация и стандартизация способов и методов защиты;

9) реализация моделей взаимного недоверия и взаимной защиты всех участников информационного обмена, включая арбитра и злоумышленника (криптоаналитика), в применяемых механизмах защиты информационного обмена (цифровой подписи, аутентификации, контроля целостности, шифрования, управления доступом и маршрутизации, автоматического протоколирования и аудита);

10) внедрение автоматизированной системы контроля и управления информационной безопасностью Системы;

11) внедрение интеллектуальной системы поддержки принятия решений по управлению безопасностью информации, которая содержит в себе свойства экспертной системы реального времени и интегрированной программной среды.

В разделе «Требования к подсистеме криптографической защиты информации КСЗИ Системы» приводятся основные требования к составу и характеристикам применяемых криптосистем, криптопротоколов, аппаратных, аппаратно-программных и программных средств криптографической защиты. Кроме этого, приводятся требования к функциональной и организационно-топологической структуре подсистемы криптографической защиты информации.

В разделе «Требования к архитектуре КСЗИ Системы» излагаются основные требования к организационной, функциональной и топологической структурам КСЗИ, составу информационного, программного и технического обеспечения. Основные требования разрабатываются с учетом концепции построения Системы, выбранной архитектуры Системы, политики безопасности информации в Системе.

В разделе «Этапы развития КСЗИ Системы» излагаются этапы разработки и внедрения КСЗИ, которые определяются в соответствии с правовыми и договорными документами, регламентирующими создание Системы.

Заключение

Материалы, помещенные в статью, разработаны с использованием действующих на момент написания статьи отечественных и зарубежных нормативных документов по обеспечению безопасности информации. Представленные в статье методологические основы концепции и политики безопасности информационных технологий отражают опыт авторов по разработке комплексных систем защиты информации различного назначения.

Список литературы: 1. Положення про порядок здійснення криптографічного захисту інформації в Україні. Указ Президента України від 22.05. 1998. N 505/98 2. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ. 1999. 3. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. ДСТСЗІ СБУ. 1999. 4. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ. 1999. 5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ. 1999. 6. НД ТЗІ 2.5-005 –99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. ДСТСЗІ СБУ. 1999. 7. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях/под редакцией В. Ф. Шаньгина. М.: Радио и связь, 1999. 328 с. 8. ISO/DIS 7498/2. Information Processing System – OSI. Reference Model. Part 2: Security Architecture. ISO. 1988. 32 p.

*Харьковский государственный университет
радиоэлектроники*

Поступила в редколлегию 5.04.2001