УДК 621.327

# ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ВОЙСКАМИ И ОРУЖИЕМ

д.т.н., проф. Ю.В. Стасев

*Предлагаются подходы к построению системы защиты информации в автоматизированной системе управления войсками и оружием.*

**Введение.** Современный этап развития системы управления Вооруженных Сил Украины характеризуется совершенствованием организационно-штатной структуры в системе управления войсками и оружием, применением новых достижений в области математического и программного обеспечения, широким использованием электронно-вычислительной техники. Использование ЭВМ, современных методов передачи, обработки и хранения информации, организация перестройки системы управления войсками и оружием нашли отражение в создании единой автоматизированной системы боевого управления (АСБУ). В основу создания и развития АСБУ положена многолетняя программа, предусматривающая последовательную и целенаправленную отработку технических решений и методов управления. По мере осознания целей и задач, стоящих перед АСБУ, наметился системный подход к планированию, использованию и разработке технического облика АСБУ. Опыт разработок и эксплуатации подобных систем за рубежом показывает, что создаваемая в Вооруженных Силах Украины АСБУ должна строиться на основе архитектуры открытых систем. Построение АСБУ на принципах открытых систем позволяет объединить в единую автоматизированную систему различные виды и рода войск и обеспечить простой доступ пользователей к корпоративной информации системы управления. Вместе с тем такое построение АСБУ выдвигает на первый план проблему безопасности информации, вычислительных компонентов, аппаратных платформ, операционных систем, баз данных и прикладного программного обеспечения различных пользователей. Проблема информационной безопасности в АСБУ состоит не только в реализации совокупности мер, характеризующих сохранность корпоративной информации от случайного или преднамеренного разрушения и несанкционированного использования, но и в согласовании работы средств защиты различных звеньев автоматизированной системы управления войсками и оружием [1 – 4].

В настоящей статье автор на основе опыта разработки и эксплуатации систем защиты информации в современных информационных системах предлагает подход к построению системы защиты информации в АСБУ.

**1. Защита информации в АСБУ.** Широкое внедрение электронно-вычислительной техники в систему управления войсками и оружием уже сегодня позволило создать пространство, в котором создается, накапливается, распределяется, передается и уничтожается информация. Бесспорным является тот факт, что использование новых информационных технологий в военном деле является безусловным преимуществом. Однако, подобно тому, как достижения ядерной физики породили угрозу ядерной войны, создание единого информационного пространства становится источником практически неразрешимых или трудноразрешимых проблем. Реальная необходимость обеспечения информационной безопасности требует создания системы защиты информации в АСБУ.

Система защиты информации предназначена для непрерывной и комплексной защиты информации в процессе информационного обмена в АСБУ с требуемыми уровнями защиты, обеспечивающими реализацию политики безопасности информации на всех этапах ее жизненного цикла с использованием передовых информационных технологий.

Ядром, определяющим концепцию построения системы защиты информации в АСБУ, является политика безопасности – выбор правил, определяющих процедуры и механизм обеспечения безопасности всего множества объектов и субъектов безопасности АСБУ.

В практическом приложении политика безопасности проявляется через совокупность документированных управленческих решений, направленных на обеспечение безопасности информации и ассоциированных с ней ресурсов. Политика безопасности реализуется в системе защиты информации в АСБУ, представляющей собой комплекс организационных мер, технических средств, юридических норм, физических ограничений, для предотвращения причинения вреда боевой готовности войск и вооружения (рис. 1).

Основными целями создания системы защиты информации в АСБУ являются [1, 4, 7]:

1. Обеспечение конфиденциальности информации и сообщений, циркулирующих в АСБУ.

2. Обеспечение целостности и подлинности приказов, распоряжений и команд, передаваемых в АСБУ.

3. Защита трафика АСБУ на сетевом уровне использованием стандартных протоколов.

4. Обеспечение надежной идентификации объектов и субъектов сети

АСБУ, а также защита от несанкционированных действий, как санкционированных, так и несанкционированных пользователей.

5. Управление ключевыми структурами на сетевом и прикладном уровне в автономном и общесистемном режиме.

6. Обеспечение ответственности пользователей АСБУ за сформированные, переданные и принятые сообщения.

7. Обеспечение помехозащищенности, имитостойкости и скрытности системы связи в АСБУ.


Рис. 1. Политика безопасности информации в АСБУ

**2. Состав и структура системы защиты информации в АСБУ.** Элементы современной автоматизированной системы боевого управления, как правило, являются главными составляющими частями сложных комплексов вооружения и характеризуются мощным математическим, программным и алгоритмическим обеспечением. Разрабатываемая система защиты информации должна обеспечивать безопасность информации во всех элементах АСБУ. Многообразие объектов и субъектов АСБУ предполагает использование большого числа подходов к обеспечению безопасности информации, а, следовательно, приводит к необходимости разработки и реализации различных методов и средств защиты информации. Вместе с тем эти различные подходы должны быть интегрирова-

ны в АСБУ с учетом единой политики безопасности. Сложность построения системы защиты информации усугубляется еще и тем, что необходимо разрабатывать и совмещать друг с другом системы безопасности информации различных структурных звеньев АСБУ. Здесь можно различить системы защиты информации видов и родов войск, региональные системы обеспечения защиты информации и единую систему обеспечения безопасности информации. Ясно, что в этом случае нельзя говорить о полном аппаратном и программном совмещении этих систем. Отсюда вытекает важность и большая значимость выработки единой идеологии обеспечения безопасности информации в АСБУ, необходимость разработки единых требований по безопасности информации, как организационных, так и технических, которые должны быть обязательными для всех субъектов АСБУ.

Высокие характеристики безопасности могут быть достигнуты при комплексном подходе к разработке системы безопасности информации. А это значит, что политика и система защиты информации должны разрабатываться параллельно с разработкой основных компонентов АСБУ. В противном случае средства защиты информации не будут интегрированы в структуру всех компонентов единой сети. Процесс проектирования и создания системы защиты информации в АСБУ должен быть многоэтапным: проведение анализа объекта защиты, с выявлением характера защищаемой информации, выявление каналов утечки и угроз, разработка и внедрение методов и средств защиты информации, оценка эффективности принятых мер по защите информации. Сущность проблемы обеспечения информации предполагает постоянный контроль, анализ и оценку эффективности используемых организационных и технических средств защиты информации, выявление незащищенных или вновь возникших каналов утечки информации и угроз. На основе полученных результатов осуществляется разработка дополнительных мер по обеспечению безопасности с целью усовершенствования системы защиты информации.

Сложность и многообразие задач, решаемых АСБУ, предполагают многофункциональность системы защиты информации. Это позволит обеспечить гибкость системы и непрерывную, комплексную защиту информации на всех этапах ее жизненного цикла с требуемым уровнем защиты.

Система защиты информации в АСБУ может состоять из рабочих станций пользователей прикладного уровня, рабочих станций (серверов) сетевого уровня, центров управления безопасностью и региональных центров управления ключами, серверов администраторов локальных и сетевых экранов (брандмауэров). Структура системы защиты информации в АСБУ приведена на рис. 2.

***1. Рабочая станция пользователя АСБУ*** на прикладном уровне должна обеспечивать: *цифровую подпись* приказов, докладов, команд, сообщений по национальным алгоритмам; *шифрование и дешифрование* приказов, докладов, команд, сообщений по национальным стандартам; *архивирование и рандомизацию* сообщений; *направленное шифрование и дешифрование* информации в системе с открытыми ключами; подготовку криптограмм для эффективной передачи по сети АСБУ; *автоматическое протоколирование* всех операций, выполняемых на рабочих станциях, *блокировку в случае несанкционированных действий* с сигнализацией на вышестоящее звено; *генерацию личных и открытых ключей*, передачу их в центр для сертификации, прием сертифицированных ключей, их запись, хранение и использование.

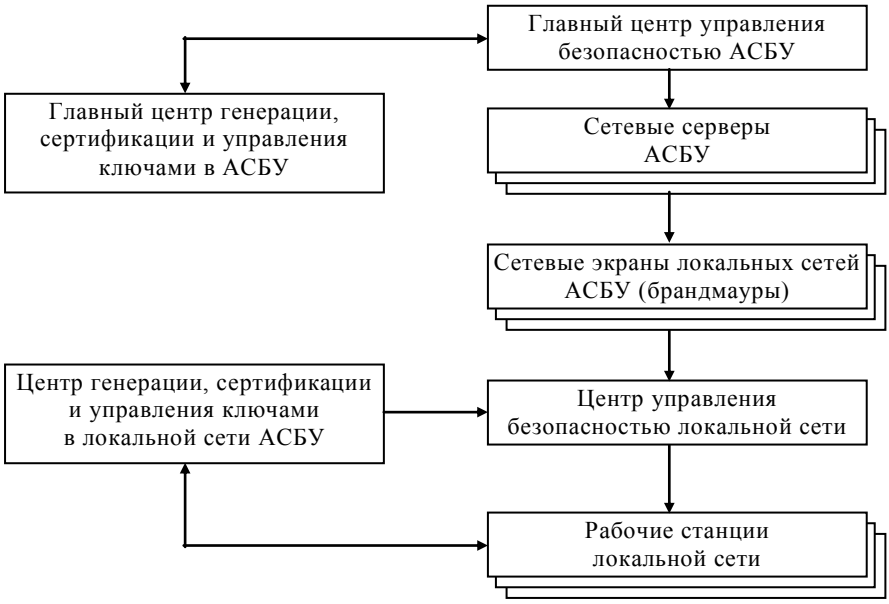


Рис. 2. Структура системы защиты информации в АСБУ

***2. Рабочая станция сетевого уровня*** должна обеспечивать: *инкапсуляцию или шифрование пакетов* на сетевом уровне с использованием стандартных протоколов; *выработку личных и открытых ключей*, передачу и прием открытых ключей после сертификации; *взаимодействие с* «видимыми» *рабочими станциями* сетевого уровня, в том числе в режиме удаления или добавления; *взаимодействие* с центрами управления безопасностью с использованием состоятельных протоколов.

***3. Центр управления безопасностью*** должен обеспечивать: *генерацию (расчет) открытых ключевых параметров* цифровой подписи; *формирование* секретных и открытых параметров ключа сертификации центра; формирование, распределение и доставку открытых ключевых параметров, открытого ключа сертификации центра, открытых и секретных ключей сертификации пользователей на соответствующие станции; создание инсталляционного именного пакета генерации ключей для каждого пользователя; сертификацию открытых ключей и передачу их на рабочие станции.

***4. Центры*** *управления безопасностью на сетевом уровне* должны обеспечивать: формирование, распределение и доставку открытых и секретных ключевых параметров и ключей сертификации на рабочие станции сетевого уровня; согласование механизмов защиты между различными ведомствами и регионами, выбор режимов работы; управление ключевыми структурами с использованием состоятельных протоколов; изменение конфигурации сети, в том числе в режимах удаления или добавления рабочих станций.

**Заключение.** Исходя из требований, предъявляемых к безопасности информации, возможности технической реализации системы защиты информации в АСБУ, требуется реализовать следующие положения:

– защите подлежит вся информация и ресурсы, представленные в АСБУ;

– защита информации производится не менее чем на двух уровнях – прикладном и сетевом;

– на прикладном уровне каждое ведомство или группа ведомств защиту информации осуществляет с разграничением по уровням секретности и ведомствам;

– для защиты информации на прикладном уровне в той или иной мере применяются механизмы аутентификации, в том числе цифровой подписи, контроля целостности и подлинности, шифрования, управления доступом, автоматического протоколирования и аудита;

– управления ключевыми структурами и безопасностью на прикладном уровне производится с ведомственных центров, которые взаимодействуют с главными и возможно региональными центрами управления безопасностью в АСБУ;

– защита трафика сети осуществляется на сетевом уровне посредством инкапсуляции пакетов с использованием высокоскоростных алгоритмов шифрования с распределением и выработкой секретных пакетов ключей по каждому направлению в системе с открытым распространением ключей;

– на начальном этапе создания сети для реализации механизмов защиты используются процедуры и алгоритмы, разрешенные для применения в Украине, а на последующих этапах и национальные, получившие соответствующие сертификаты;

– процедуры и алгоритмы, в зависимости от финансовых возможностей Украины, могут быть реализованы программно, программно-аппаратно или аппаратно;

– защита информации, в том числе управление доступом в выделенных локальных сетях производится специальным сервером-администратором;

– защита локальных сетей от угроз извне производится с использованием специальных экранов (брандмауэров);

– процедуры идентификации, аутентификации и обмена ключами реализуются с использованием состоятельных протоколов;

– в отдельных локальных сетях и ведомствах на прикладном уровне может осуществляться несколько процедур цифровой подписи, управления доступом и шифрования;

– параметры процедур и алгоритмов защиты информации выбираются с учетом допустимых рисков и ограничений с использованием соответствующих показателей;

– на всех уровнях осуществляется обработка кодов возврата преобразований, которые фискально доступны соответствующим центрам управления безопасностью.

Представленные концептуальные основы построения системы защиты информации могут быть взяты за основу при разработке политики безопасности и системы защиты информации в АСБУ.

## ЛИТЕРАТУРА


1. *Герасименко В.А. Основы теории защиты информации в автоматизированных системах обработки данных. – М., 1991. Деп. В ВИНИТИ. – № 1080В91. – 1991.*
2. *Вербицький М.І. Вступ до криптології. – Львів: Світоч, 1997.*
3. *Стенг Д., Мун С. Секреты безопасности сетей. – К: Диалектика, 1995. – 544 с.*
4. *Мафтик С. Механизмы защиты в сетях ЭВМ. – М: Мир, 1993. – 216 с.*
5. *Закон Украины «О защите информации в автоматизированных системах» от 5 июня 1994 г. // Безопасность информации. – 1995.– № 1. – С. 56 – 62.*
6. *Ушаков Л.М. Принципы построения систем управления безопасностью данных в информационно-вычислительных сетях. // АиВТ. – 1994. – № 4. – С. 11 – 17.*
7. *Моисеенков И. Арифметическая классификация и принципы оценивания безопасности компьютерных систем // Безопасность компьютерных систем. – № 3. – 1996. – С. 23 – 29.*


*Поступила 23.06.2003*

***СТАСЕВ Юрий Владимирович**, доктор технических наук, профессор, начальник факультета ХВУ. Окончил ХВВКИУ в 1981 году. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*