# Раздел I
# Фундаментальные проблемы информационной безопасности

**Ю.В. Бородакий, А.Ю. Добродеев**
Россия, г. Москва, ФГУП «Концерн “Системпром”»

## ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

В соответствии с Концепцией национальной безопасности Российской Федерации национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Вместе с тем в данном документе подчеркивается усиление угроз национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Таким образом, в настоящее время информационная безопасность имеет особое значение для обеспечения национальной безопасности государства. В Российской Федерации решение проблем обеспечения информационной безопасности осуществляется в соответствии с положениями Доктрины информационной безопасности Российской Федерации. Данный документ определяет, что одной из составляющих национальных интересов Российской Федерации в информационной сфере является защита информационных ресурсов от несанкционированного доступа (НСД), обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Следовательно, решение задач обеспечения информационной безопасности Российской Федерации требует использования в качестве основы информационной и телекоммуникационной инфраструктуры России защищенных автоматизированных систем (АС). Опыт разработок ФГУП "Концерн "Системпром" показал, что создание защищенных АС, т.е. систем удовлетворяющих определенным требованиям по обеспечению безопасности информации, возможно лишь на основе комплексного подхода, заключающегося в рациональном сочетании следующих составляющих:

- защита от утечки по техническим каналам и противодействие техническим средствам разведки;
- применение аппаратно-программных средств защиты информации для создания системы защиты информации (СЗИ) от НСД;
- разработки и реализация комплекса организационно-технических мер.

Следует учесть, что третья составляющая должна лишь компенсировать недостатки в реализации первых двух. Решение задач в рамках первой составляющей

осуществляется на основе применения активных и пассивных технических средств, разрабатываемых на основе известной теоретической базы.

Решение задач обеспечения информационной безопасности в рамках второй составляющей регламентируется Руководящими документами ФСТЭК России. Изложенные в названных руководящих документах требования определяют функции, которые должны быть реализованы в соответствующих механизмах системы защиты информации (СЗИ).

Наиболее жестко эти требования сформулированы и предъявляются к средствам и системам, предназначенным для обработки информации составляющей государственную тайну с максимальным грифом. Вместе с тем, изложенные в Руководящих документах требования не учитывают специфики реализации предъявляемых к механизмам защиты информации требований в конкретных информационных технологиях.

Тем не менее, в процессе создания защищенных автоматизированных систем отечественные разработчики сталкиваются с целым рядом проблем, решение которых требует объединения и координации усилий различных специалистов на государственном уровне.

Важнейшей из таких проблем является создание теории информационной безопасности распределенных автоматизированных систем. Накопленный в настоящее время ФГУП "Концерн "Системпром" значительный опыт решения практических задач по созданию защищенных автоматизированных систем по заказу федеральных органов исполнительной власти, в том числе и силовых, позволяет утверждать, что наряду с требующими решения фундаментальными научными проблемами существует не меньшее число проблем, носящих прикладной характер.

Анализ нынешнего состояния существующих и создаваемых защищенных автоматизированных систем позволяет утверждать, что наличие названных проблем обусловлено в первую очередь территориальной распределенностью защищаемых автоматизированных систем и использованием для решения функциональных задач разнообразных информационных технологий, созданных различными разработчиками. В конечном итоге, автоматизированные системы представляют собой сложные и разветвленные структуры, состоящие из множества различных элементов.

Для обеспечения нормального функционирования подобных структур необходимо в любой момент времени иметь актуальную информацию о работоспособности ее элементов, т.е. о текущем состоянии программных и аппаратных средств, иметь возможность удаленного диагностирования и управления изменением настроек этих средств. Все это приводит к усложнению системы управления средствами защиты информации и увеличению роли антропогенного фактора в снижении эффективности современных СЗИ АС.

Опыт разработок концерна показал, что существенное увеличение эффективности применения средств из состава СЗИ возможно лишь при условии решения проблемы создания адаптивных СЗИ, в которых реализованы методы интеллектуальной обработки данных. Основной задачей названных СЗИ должно являться формирование управляющих воздействий на средства защиты информации при изменении условий функционирования АС.

Следует отметить, что в настоящее время существуют примеры успешных практических реализаций автоматического изменения настроек средств защиты информации при выявлении изменения условий функционирования АС (например, при обнаружении информационного воздействия нарушителя на АС). Наибольшие

успехи в данной области достигнуты при разработке межсетевых экранов и систем предотвращения вторжений.

В рамках решения данной проблемы необходима разработка и внедрение общепринятого метода количественной оценки уровня защищенности информации в АС. Анализ текущего состояния работ в названной области позволяет констатировать наличие определенных положительных результатов. Разработан целый ряд методов анализа рисков, вероятностных методов оценивания защищенности информации, методов оценивания уровня защищенности информации в АС на основе теории игр.

Однако каждый из этих методов имеет определенные недостатки, препятствующие их полноценной практической реализации в СЗИ АС для определения уровня защищенности информации. Как правило, названные недостатки обусловлены сложностью получения значений некоторых величин. Например, степени опасности угрозы, степени ослабления угрозы средством защиты информации и т.д.

Опыт специалистов в области разработки защищенных АС позволяет утверждать, что неформальное выполнение требований по обеспечению безопасности информации в АС невозможно без создания защищенной сетевой инфраструктуры АС. Наличие такой инфраструктуры особенно актуально в связи с нарастающими темпами разработки и внедрения информационных технологий, обеспечивающих передачу всех видов коммуникационного трафика на основе применения IP сетей. В настоящее время существует множество отечественных аппаратно-программных средств, предназначенных для защиты информации, передаваемой по сети.

Однако разработки подобных средств ведутся в условиях отсутствия единой концепции защищенной сетевой инфраструктуры, которая была бы утверждена в соответствующих руководящих документах. В рамках данной концепции должны быть регламентированы все аспекты создания защищенной сетевой инфраструктуры:

– разработка спецификаций сетевых протоколов, особенно протоколов прикладного уровня, с учетом требований по обеспечению безопасности информации;

– разработка структуры и архитектуры защищенной сети;

– разработка аппаратного и программного обеспечения, компонентов ОС и прикладного программного обеспечения, предназначенных для создания защищенной сетевой инфраструктуры АС и т.д.

И в заключение необходимо остановиться на одной важнейших составляющих, оказывающих значительное влияние на уровень защищенности информации в АС. Существующая система сертификации АС на соответствие требованиям по обеспечению безопасности информации практически не учитывает влияние прикладного программного обеспечения на выполнение этих требований, поскольку они предъявляются именно к механизмам защиты информации. Особую значимость данная проблема приобретает при наличии компонент прикладного программного обеспечения, функционирующих в контексте привилегированных учетных записей.

Многие разработчики прикладного программного обеспечения вообще не акцентируют внимание на обеспечении безопасности информации. Следствием наличия подобных недостатков проектирования становится привнесение в АС уязвимостей, существенно снижающих уровень защищенности информации в АС, обнаружение и эксплуатация которых может позволить нарушителю осуществить НСД к информации в обход средств защиты информации из состава СЗИ АС.

Решение рассмотренной проблемы должно основываться на утвержденной соответствующими руководящими документами технологии разработки про-

граммного обеспечения для защищенных АС, учитывающей различные аспекты обеспечения безопасности информации на всех этапах разработки.

Предложения ФГУП «Концерн “Системпром”» в части создания перспективных подсистем СЗИ для АС ВН таковы:

| **Название подсистемы** | **Состав и основные функции** |
|---|---|
| **Подсистема обнаружения атак** | средства сбора информации о контролируемых параметрах АС;<br>средства обнаружения атак;<br>средства идентификации атак и обучения обнаружению новых атак |
| **Подсистема извлечения и накопления знаний** | средства сбора данных о методах и средствах атак, с использованием технологий создания ложных объектов атаки;<br>средства предварительного анализа, структуризации и хранения знаний об уязвимостях АС и атаках |
| **Подсистема анализа защищенности** | средства сбора информации о параметрах АС;<br>средства анализа и получения количественных показателей уровня защищенности АС |
| **подсистемы адаптации СЗИ** | средства принятия решения для формирования сигналов управления;<br>средства регулирования параметров СЗИ АС |
| **Подсистема активного противодействия атакам** | средства выбора оптимальной стратегии противодействия;<br>средства активного воздействия на процесс совершения атаки |
| **Подсистема маскировки сегментов и элементов сети АС ВН** | средства скрытия сегментов и элементов сетей АС ВН, с целью нейтрализации воздействия противоборствующей стороны на АС ВН;<br>имитация сегментов и элементов сетей АС ВН, с целью выявления, оценки и прогнозирования угроз Российской Федерации и ее Вооруженным Силам в информационной сфере;<br>дезинформация и демонстративные действия, с целью введения противоборствующей стороны в заблуждение относительно состава, положения, состояния, предназначения и характера деятельности АС ВН |

**Л.К. Бабенко, В.Г. Захаревич, О.Б. Макаревич**
Россия, г. Ростов-на-Дону, Южный федеральный университет
г. Таганрог, Технологический институт ЮФУ

## СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ РЕАЛИЗАЦИЯ В НАУЧНОЙ И ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

В докладе рассматриваются некоторые проблемы информационной безопасности и их реализация в рамках учебного процесса на кафедре безопасности информационных технологий ТТИ ЮФУ и при выполнении соответствующих НИ-