УДК 004.415.056.5 **С.В. Толюпа, В.С. Наконечный, М.М. Ковбель**

# УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ СИСТЕМНОГО АНАЛИЗА

В статье показано, что методологические основы управления защитой информации в сегменте локальной информационной системы, базируются на системном анализе и общих закономерностях построения систем управления, решение которых заключается в совокупности разработанных методов, принципов построения архитектуры системы управления защитой информации с интеллектуальной поддержкой организационно-технического и оперативного управления, что позволяет принимать оперативные и обоснованные решения для обеспечения требуемого уровня защищенности информации.

***Ключевые слова:*** защита, системный анализ, система, информация, информационная безопасность, угроза, локальная сеть.

## Введение

Новый этап в развитии обмена информацией, который характеризуется интенсивным внедрением современных информационных технологий (ИТ), широким распространением локальных, корпоративных и глобальных сетей, создает новые возможности и качество информационного обмена.

Сегодня нельзя представить развитие любого предприятия без эффективной информационной системы. Однако, применение ИТнемыслимо без повышенного внимания к вопросам информационной безопасности (ИБ) из-за наличия угроз защищенности информации.

Приблизительно структура последствий неэффективного обеспечения ИБ в американских организациях такова: кража конфиденциальной информации – 20-25% от общего годового убытка; фальсификация финансовой информации – 21-25%; загрязнение вредоносными программами – 11-12%; нарушение доступа к Web-страницам – 1-11%; срыв работы информационной системы (ИС) – 4-10%; незаконный доступ пользователей к информации – 4-9%; другие виды нарушений – 14-33%. В таких условиях всё больше распространяется аксиома, что защита информации должна по своим характеристикам быть соответствующей масштабам угроз. Отход от этого правила приведёт к дополнительным убыткам. Для каждой ИС имеется оптимальный уровень защищённости, который необходимо постоянно поддерживать.

Нет сомнений, что защита критически важных для ИС массивов соответствует международным, корпоративным, нормативным и методическим документам. Используются дорогостоящие технические средства и внедряются строго регламентированные организационные мероприятия. Однако нет ответа на самый важный вопрос – насколько предложенные и реализованные решения действительно хороши, какова их планируемая и реальная эффективность. Такому положению, имеющемся в ИС, но нежелательному в области ИБ есть ряд причин [1]:

– игнорирование системного похода к методологии анализа и синтеза построения систем защиты информации (СЗИ);

– отсутствие механизмов полного и достоверного подтверждения качества СЗИ;

– недостатки нормативно-методического обеспеченияІБ, прежде всего в области показателей и критериев.

Прежде всего, СЗИ должна иметь целевое назначение. Причём, чем более конкретно сформулирована цель защиты информации, детально выяснены имеющиеся ресурсы, и определён комплекс ограничений, тем в большей степени возможно получение положительного результата. Когда цель обеспечения информационной безопасности проста и принципиально достигается, то достаточно несложных по структуре СЗИ. Однако, при расширении круга решаемых проблем для обеспечения ИБ, содержание целевого назначения системы на формализованному уровне определяет многомерный, векторный характер. При

этом важность свойств отдельных элементов СЗИ понижается и на первый план выходят общесистемные задачи – определение оптимальной структуры и режимов функционирования системы, организация взаимодействия между элементами системы, учёт воздействий внешней среды и т.д. При целенаправленном объединении элементов в систему последняя требует специфических свойств, которые не имеются ни в одной из её элементов, частей. При системном подходе первостепенное значение имеют только те свойства элементов, которые определяют взаимодействие друг с другом и не воздействуют на систему в целом, а также на достижение поставленной цели.

Для современного этапа развития теории и, в особенности, практики обеспечения защиты информации (ЗИ) характерна парадоксальная ситуация. С одной стороны, усиленное внимание к безопасности информационных объектов, существенное повышение требований по ЗИ, принятие международных стандартов в области ИБ, постоянно растущие расходы на обеспечение защиты. С другой стороны – столь же неуклонно растущий ущерб, причиняемый собственникам и владельцам информационных ресурсов, о чем свидетельствуют регулярно публикуемые данные об ущербе мировой экономике от компьютерных атак. Очевидно, что современные подходы к организации ЗИ не в полной мере обеспечивают выполнение требований по ее защите. Основные недостатки использующихся повсеместно СЗИ определяются сложившимися жесткими принципами построения архитектуры и применением в основном, оборонительной стратегии защиты от известных угроз. Критичная ситуация в сфере ИБ усугубляется в связи с использованием глобальной сети для внешних и внутренних электронных транзакций предприятия и появлением неизвестных ранее типов деструктивных информационных воздействий.

Поэтому для успешного использования современных ИТ необходимо эффективно управлять не только сетью, но и СЗИ, при этом на уровне ИС автономно должна работать система, реализующая управление составом событий ИБ, планирование модульного состава СЗИ и аудит. Поскольку объект управления – СЗИ является весьма сложной организационно-технической системой, функционирующей в условиях неопределенности, противоречивости и неполноты знаний о состоянии информационной среды, управление такой системой должно быть основано на применении системного анализа, методов теории принятия решений и необходимой интеллектуальной поддержки [2]. Вместе с тем в области разработки методов и систем защиты информации в настоящее время практически отсутствуют исследования, направленные на обеспечение автоматизированной поддержки управления ЗИ для решения проблемы обеспечения требуемого уровня защищенности информации в течение всего периода функционирования СЗИ.

**Основная часть**

Одним из вариантов решения данной проблемы является использование методов интеллектуальной поддержки принятия решений в управлении ЗИ в сегменте локальной информационной системы, что в свою очередь, требует разработки на основе принципов системного анализа и общенаучных подходов методологических основ управления защитой информации, соответствующих моделей, методов, алгоритмов и программного обеспечения [3].

Таким образом, целью статьи является разработка системы управления защитой информации в сегменте локальной информационной системы для решения научно-практической задачи обеспечения требуемого уровня защищенности информации в течение жизненного цикла системы защиты информации в условиях неопределенности информационных воздействий с использованием интеллектуальной поддержки принятия решений на основе системного анализа.

Анализ соответствующих зарубежных и отечественных публикаций позволил выявить растущую популярность средств оценки риска, программных комплексов анализа и управления рисками. Анализируются представленные на рынке программные продукты для

автоматизации управления рисками нарушения ИБ. Показано, что недостатками этих систем являются: необходимость наличия экспертов высокой квалификации; трудности, возникающие при адаптации методов к потребностям конкретной организации; невозможность оценить эффективность конкретного комплекса средств защиты, применяемого на объекте защиты; требование наличия на предприятии достоверной статистики по инцидентам ИБ.

Проведенный анализ существующих стандартов в области менеджмента ИБ позволяет сделать вывод о том, что целью стандартов является формирование общих понятий и этапов управления. Вместе с тем, стандарты не формируют конкретных подходов к управлению безопасностью, они определяют функциональные требования в отношении средств защиты и не предлагают методик сравнительного анализа различных комплексов средств защиты в целях выявления наиболее рационального варианта СЗИ.

Для реализации упреждающей стратегии защиты в СЗИ сегмента локальной ИС обосновывается необходимость разработки практически применимых моделей и методов интеллектуальной поддержки планирования рационального модульного состава СЗИ, оценки и прогнозирования риска нарушения ИБ и управления ЗИ в условиях неопределенности информационных воздействий.

Главным направлением поиска путей ЗИ является неуклонное повышение системности подхода к самой проблеме защиты информации. Понятие системности интерпретировалось прежде всего в том смысле, что ЗИ заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для ЗИ, непременно и наиболее рационально объединяются в единый целостный механизм - систему защиты [4].

Основные трудности реализации систем защиты (СЗ) состоят в том, что они должны удовлетворять двум группам противоречивых требований. С одной стороны, должна быть обеспечена надежная защита находящейся в системе информации, что в более конкретном выражении формулируется в виде двух обобщенных задач: исключение случайной и преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала. С другой стороны, СЗ не должны создавать заметных неудобств в процессе работы с использованием ресурсов системы. В частности должны быть гарантированы полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий. К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у пользователей современных ИС.

Основываясь на принципах системного анализа, который представляет собой теорию и практику улучшающего вмешательства в проблемную ситуацию, предлагается вариант декомпозиции проблемы разрешения имеющихся противоречий в области обеспечения безопасности информации [5].

На основании системного подхода показано, что модель проблемной ситуации в области ЗИ содержит совокупность трех взаимодействующих систем: проблемосодержащей СЗИ; проблемо-разрешающей управляющей системы, которая разрабатывается для того, чтобы исключить или уменьшить проблему, окружающей, или существенной среды, с которой взаимодействует СЗИ, под которой понимается множество потенциально возможных угроз ИБ. Требование постоянно нарастающей детализации приводит к построению модели состава проблемосодержащей системы, модели объекта защиты и модели угроз.

Следует отметить, что основной проблемой при построении управляющей системы является разработка модели угроз, что связано со специфичностью взаимодействия объекта

управления – СЗИ с окружающей средой. В связи с этим предлагается концепция построения модели угроз безопасности информации, базирующаяся на разрабатываемой классификационной схеме преднамеренных целенаправленных угроз информационной среде локальной ИС. Показывается целесообразность построения совокупности моделей: функциональной, на основе описания последовательности действий злоумышленника (нарушителя) с помощью деревьев угроз, и пространственной графовой, систематизированных в формате интегральной структурной модели каналов несанкционированного доступа, утечки и деструктивных воздействий, позволяющей провести всесторонний анализ реальных угроз, повысить адекватность модели угроз для конкретного объекта защиты. Разрабатываются деревья угроз при удаленном вторжении через сети открытого доступа, по беспроводному каналу связи, а также в случае локального сетевого вторжения нарушителя.

На основе анализа принципов управления в условиях неопределенности предлагается обобщенная архитектура системы управления ЗИ в сегменте локальной ИС. Анализируются основные функции управления, обосновывается целесообразность варианта построения системы, включающего две функциональные подсистемы: подсистему организационно-технического управления и подсистему оперативного управления в реальном масштабе времени. В соответствии с требованием количественной оценки характеристик систем, выдвигаемым системотехникой, в качестве управляемой переменной вводится показатель – уровень защищенности, требуемое значение которого зависит от максимального уровня критичности обрабатываемой в данный период времени информации.

В контуре организационно-технического управления создаются механизмы управления ЗИ при изменении инфраструктуры, бизнес-приложений, планов обработки информации и соответствующих им требований к уровню защищенности информации. Контур включает: систему интеллектуальной поддержки принятия решений по выбору стратегии защиты, систему оценки уровня защищенности (риска), управляющее воздействие реализуется сотрудниками отдела ИБ. Командная информация формируется в ходе планирования – целенаправленного выбора рационального комплекса СЗ.

В контуре оперативного управления формируется оперативная командная информация, которая доводится до объекта управления администратором безопасности или автоматически с помощью средств реализации управляющих воздействий на встроенные в средства защиты управляющие модули.

В системе управления, имеющей такое архитектурное построение, эффективные решения выбираются и принимаются как на основе сведений о технических характеристиках средств защиты, так и на основе анализа контролируемого пространства.

Архитектура системы управления защитой информации в сегменте локальной информационной системы показана на рисунке 1.

На основе анализа возможностей совершенствования управления ЗИ за счет применения новых методов решения задач управления и сокращения длительности цикла управления разрабатывается функциональная модель системы управления в позволяющая наглядно и эффективно отобразить механизм управления ЗИ, выявить процессы, для реализации которых необходима разработка автоматизированной системы интеллектуальной поддержки управления.

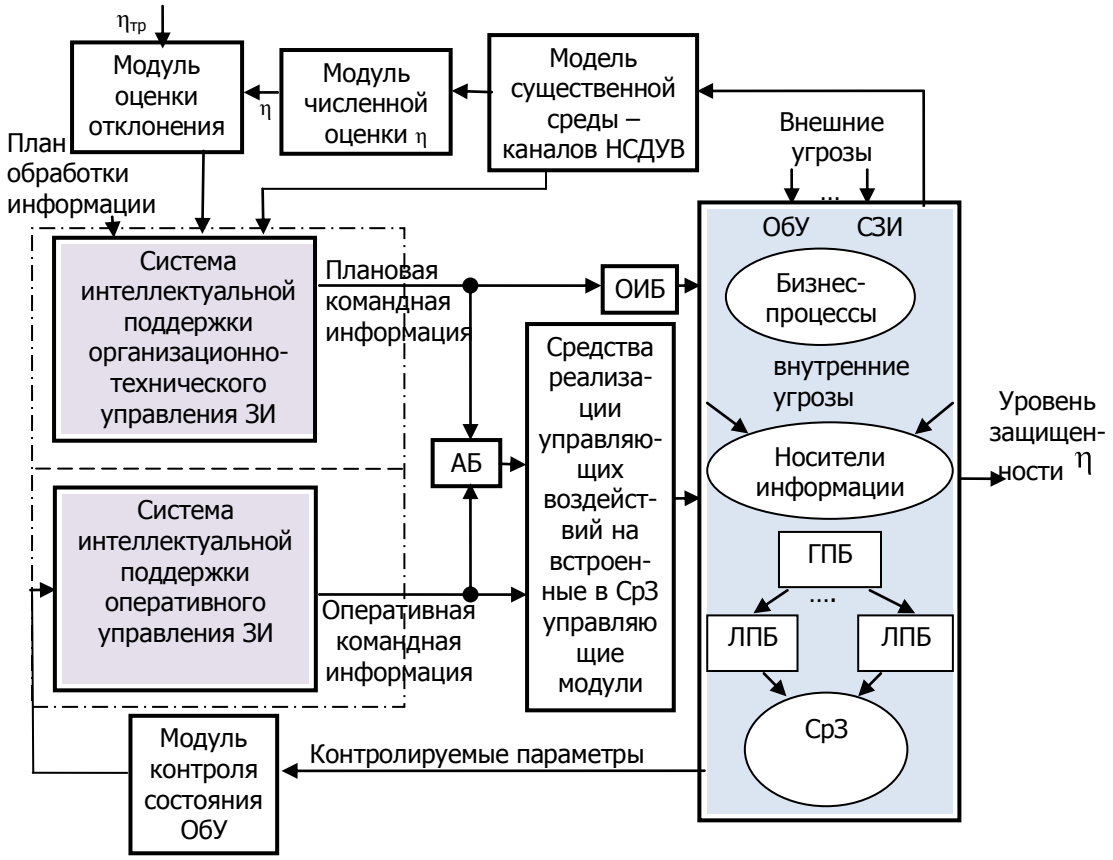


Рис. 1. Архитектура системы управления защитой информации в сегменте ЛИС: АБ – администратор безопасности; ОИБ – сотрудники отдела информационной безопасности; ОбУ (СЗИ) – объект управления; ГПБ, ЛПБ – глобальная, локальные политики безопасности; НСДУВ – несанкционированный доступ, утечка, деструктивное воздействие; СрЗ – средства защиты; $\eta_{тр}$ – требуемое значение уровня защищенности

**Выводы**

Таким образом можно утверждать, что основы управления ЗИ в сегменте локальной информационной системы, базируются на системном анализе и общих закономерностях построения систем управления, новизна которых заключается в совокупности разработанных методов, принципов построения архитектуры системы управления защитой информации с интеллектуальной поддержкой организационно-технического и оперативного управления, что позволяет принимать оперативные и обоснованные решения для обеспечения требуемого уровня ЗИ.

**Литература**

1. Андреев В.И. Проектирование систем технической защиты информации / В.И. Андреев, Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов, В.А. Хорошко–Севастополь.: Изд. Центр СНУЯЭиП, 2011. – 235с.

2. Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов. Науково-технічний журнал “Сучасний захист інформації” - К. : ДУТ, 2015. – С.34-52.

3. Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защити информационных системах. / Научно-технический журнал “Сучасний захист інформації”.– К.: ДУТ, 2012. - №4. – С. 69-74.

4. Толюпа С.В. Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації. / С.В.Толюпа, І.М. Павлов // Науково-технічний журнал “Сучасний захист інформації”.– К.: ДУТ, 2014. - №2. – С. 96-104.

5. Цвиркун А. Д. Основы структуры синтеза сложных систем. – М.: Наука, 1982. – 186 с.

Надійшла 17.01.2016 р. Рецензент: д.т.н., проф. Хорошко В.О.