Раздел I. Концептуальные вопросы информационной безопасности

УДК 001.8+007.5

В.И. Васильев, Б.Г. Ильясов, Т.А. Иванова

МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЛОЖНЫХ ОРГАНИЗАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ТРИАДНОГО ПОДХОДА

Современная научная парадигма базируется на системном подходе, согласно которому исследуемый объект рассматривается как система, состоящая из множества взаимосвязанных и взаимодействующих элементов, образующих единое целое. Многие понятия «система» базируются на тернарных отношениях или на триадах как трехэлементных множествах. Триада отражает системный закон строения мира: любая триада содержит в себе бесконечное количество триад, с другой стороны, она может бесконечно расширяться, так как каждая триада находится внутри еще большей триады. Системные триады создаются тремя элементами одного уровня, каждый из которых может служить мерой совмещения двух других. Рассматривается применение триадного подхода для разработки методологии обеспечения безопасности сложных организационных систем. Под безопасностью сложной организационной системы при этом понимается состояние защищенности ее ресурсов (элементов) от внутренних и внешних угроз. На основе триадного подхода, методология обеспечения безопасности рассматривается с трех сторон: как соединение триад, образующих жизненный цикл обеспечения безопасности, как учение о системной логической организации, объектов, средств, технологий обеспечения безопасности, а также как иерархическая модель, объединяющая используемые на различных этапах жизненного цикла обеспечения безопасности подходы и методы.

Методология; триадный подход; система организационно-технического управления; эффективность; риск.

V.I. Vasilyev, B.G. Ilyasov, T.A. Ivanova

METHODOLOGY OF PROVIDING OF COMPLEX ORGANIZATIONAL SYSTEMS SECURITY ON BASIS OF TRIAD APPROACH

Modern scientific paradigm is based on a systematic approach according to which the object is considered as a system, consisting of a set of interrelated or interacting elements forming a whole one. Many of the concepts of "system" is based on ternary relations or triads as a three-piece sets. Triad reflects the structure of the world system law: any triad contains an infinite number of triads, on the other hand, it can expand indefinitely, since each triad is in even greater triad. System triad are three elements of the same level, each element can serve as a measure of the alignment of the other two. This paper considers the application of triadic approach to develop a methodology of complex organizational systems security providing. The security of complex organizational system (COS) is the state of protection of its resources (elements) from internal and external threats. In terms of the triadic approach, security providing methodology is considered from three sides: as a compound of triads, forming security system lifecycle, as the doctrine of security technology logical organization, facilities and equipment, and as a hierarchical model that combines different security approaches and methods at each stages of the lifecycle.

Methodology; triad approach; system of organizational and technical management; efficiency; risk.

Введение. Являясь субъектами рыночной экономики, современные сложные организационные системы (СОС) вынуждены реализовывать свою деятельность в условиях конкуренции на различных рынках – услуг, трудовых ресурсов, инвестиций, инноваций и технологий, использования земли, имущества и т.п. Наличие у них эффективно функционирующей системы управления комплексной безопасностью является немаловажным преимуществом перед другими предприятиями-конкурентами. Необходимость повышения эффективности деятельности СОС связана с актуальной для любого субъекта экономики проблемой дефицита ресурсов – финансов, квалифицированных кадров, оборудования, площадей и т.п. Поэтому меры по повышению эффективности использования имеющихся ресурсов определяют методы и механизмы достижения наилучших результатов при имеющихся ресурсных ограничениях [1]. В данных условиях система управления безопасностью СОС должна и может стать органичной частью системы менеджмента качества деятельности СОС, одной из целей которой является снижение ущерба от воздействия на ресурсы дестабилизирующих факторов, а, следовательно, экономия денежных средств.

В современных условиях повышенной террористической угрозы, обостренной конкурентной борьбы, проблема управления безопасностью больших предприятий, организаций и учреждений (которые, несомненно, относятся к СОС) становится особенно актуальной. Подобные объекты, как правило, представляют собой большие, территориально распределенные организационные системы, в которых работают и (или) временно находятся тысячи людей. Отдельные подразделения (филиалы, элементы инфраструктуры и др.) и объекты (производственные корпуса, склады и др.) таких сложных организационных объектов могут находиться на значительном расстоянии друг от друга и действовать в разных условиях. В связи с этим в настоящее время проблема управления безопасностью сложных организационных объектов (СОО) стоит довольно остро, особенно вследствие того, что данной тематике до сих пор уделено не так много внимания в теории обеспечения безопасности.

Методология обеспечения безопасности СОС. *Управление безопасностью* СОО заключается в последовательном воздействии на объект управления (СОО) с целью достижения им желаемого состояния защищенности. *Состояние защищенности*, при этом, понимается как умение и способность составляющих системы безопасности надежно противостоять любым злоумышленным попыткам нанести ущерб ресурсам, подлежащим защите [2]. Следует отметить, что управление безопасностью СОО имеет две взаимосвязанных составляющих: организационную и техническую. То есть целенаправленные воздействия, которым подвергается СОО, могут иметь вид организационных мер (специальные мероприятия, регламенты, инструкции и пр.), или же управление безопасностью может осуществляться путем применения тех или иных технических средств безопасности. В связи с этим систему управления безопасностью СОО имеет смысл рассматривать как систему организационно-технического управления. *Система организационно-технического управления (СОТУ) безопасностью СОО* – это часть общей системы управления СОО, направленная на создание, обеспечение, управление, мониторинг, контроль, поддержание и улучшение комплексной безопасности СОО [3]. Как следует из данного определения, в качестве объекта управления СОТУ выступает система обеспечения комплексной безопасности СОО. Как было отмечено выше, система управления безопасностью СОО является необходимым элементом системы менеджмента качества СОО. Глобальная же система менеджмента качества деятельности СОО имеет своим объектом управления сам СОО.

При этом если в области организационной составляющей системы организационно-технического управления безопасностью накоплен обширный опыт практической работы (разработаны и применяются большой объем различных нормативных документов, регламентов, инструкций и т.д.), то ситуация, сложившаяся с технической частью данной подсистемы, характеризуется рядом проблем. Это:

- недостаточная оснащенность техническими средствами обеспечения безопасности СОО различного уровня;
- значительный физический и моральный износ существующего оборудования обеспечения безопасности;
- отсутствие специализированной подготовки у лиц, ответственных за безопасность СОО, позволяющей грамотно и оптимально распределить выделяемое на обеспечение безопасности целевое финансирование.

Таким образом, проблема разработки методологического обеспечения для процесса обеспечения и управления безопасностью СОО является актуальной.

Рассмотрим применение триадного подхода для решения указанной проблемы. С точки зрения данного подхода, методология рассматривается со следующих трех сторон [4]:

1) как учение о процессе движения к цели, т.е. рассматривается жизненный цикл такого движения;
2) как учение о системной логической организации, объектов, средств, технологий, необходимых для достижения цели;
3) как учение о процессе получения новых знаний на основе существующих научных подходов.

Построим модель жизненного цикла обеспечения безопасности сложного организационного объекта (рис. 1). Каждому из этапов этого жизненного цикла будет соответствовать своя триада.

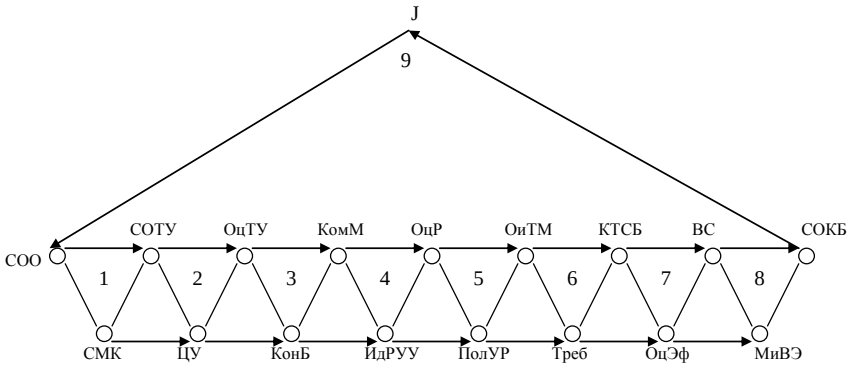

Рис. 1. Жизненный цикл обеспечения безопасности

Этап 1. Допустим, у нас имеется сложный организационный объект (СОО), безопасность ресурсов которого нам необходимо обеспечить. Состояние защищенности данных ресурсов от различных дестабилизирующих факторов напрямую является одной из составляющих общего качества функционирования СОО, а, следовательно, безопасность СОО – одна из целей системы менеджмента качества (СМК). Рассматривая процесс обеспечения безопасности СОО, неизбежно приходится выделять из СМК в целом ее компоненту, связанную как раз с безопасностью СОО, а именно с управлением обеспечением безопасности СОО. Данную составляющую выше мы назвали системой организационно-технического управления безопасностью (СОТУ). Таким образом, рассматривая процесс обеспечения

безопасности СОО, в дальнейшем нам следует сконцентрировать свое внимание именно на СОТУ. Таким образом формируется триада «сложный организационный объект – система менеджмента качества – система организационно-технического управления безопасностью».

Этап 2. Для того чтобы разработать СОТУ безопасностью, для начала необходимо определить целевой уровень обеспечения безопасности (ЦУ). Достижение данного уровня для СОО будет являться целью управления безопасностью, т.е. тем, ради чего вообще создается СОТУ. ЦУ объекта зависит от его категории, т.е. от комплексной оценки состояния объекта, учитывающей его экономическую или иную (например, культурную) значимость в зависимости от концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны. Например, можно выделить 4 категории СОО в зависимости от значимости объекта: низкая, средняя, высокая, очень высокая категории. Требования по обеспечению определенного уровня безопасности (достижению определенного рейтинга) СОО будут предъявляться в зависимости от его категории. Чем выше категория СОО, тем более высокий рейтинг он должен иметь. После категорирования СОО и определения ЦУ обеспечения безопасности, необходимо провести качественную оценку текущего состояния обеспечения безопасности (ОцТУ). Для оценки уровня обеспечения безопасности могут использоваться групповые и частные показатели безопасности. Путем заполнения специальных анкет определяется, каков текущий уровень обеспечения безопасности СОО. Мы получаем триаду «система организационно-технического управления безопасностью – целевой уровень обеспечения безопасности – оценка текущего состояния обеспечения безопасности».

Этап 3. При отклонении значения текущего уровня безопасности ОцТУ от желаемого значения ЦУ возникает необходимость в приведении текущего уровня к целевому. Первым шагом для этого является разработка *концепции обеспечения комплексной безопасности* СОО (КонБ). Данная концепция представляет собой научно обоснованную систему взглядов, определяющих основные направления, условия и порядок практического решения задач защиты ресурсов СОО от противоправных действий. В концепции обеспечения комплексной безопасности приводятся принципы организационно-технического управления безопасностью СОО, раскрывается содержание каждого этапа жизненного цикла СОТУ, приводятся результаты этапов. На основе концепции обеспечения безопасности формируется комплекс мероприятий по совершенствованию СОТУ (КомМ). При этом для каждой из групп показателей безопасности разрабатываются соответствующие мероприятия, повышающие значение соответствующего группового показателя и уровня безопасности в целом. Сформирована триада «оценка текущего состояния обеспечения безопасности – концепция обеспечения безопасности – комплекс мероприятий по совершенствованию СОТУ».

Этап 4. После того как основные направления решения задачи обеспечения безопасности СОО были определены в КонБ и разработан комплекс мероприятий КомМ по ее реализации, необходимо детализировать, по отношению к каким ресурсам СОО необходимо применять меры обеспечения безопасности, определить, от каких актуальных угроз защищать ресурсы, а также выявить слабые места СОО, то есть произвести идентификацию ресурсов, угроз и уязвимостей (ИдРУУ). Традиционно выделяют три вида ресурсов объекта, подлежащих защите: материальные (оборудование, помещения, офисная техника, телекоммуникации и т.д.), информационные (в бумажном и электронном виде), а также людские (персонал, посетители). Определяются местоположение ресурсов, их ценность. Несомненно, что ценность человеческой жизни трудно переоценить и обеспечение безопасности

людей ставится всегда на первое место. Для выделенных типов ресурсов характерны свои наборы воздействующих угроз. Источник угрозы может иметь как внутреннюю, так и внешнюю локализацию. Различают также случайные угрозы (пожары, аварии, непреднамеренная порча или уничтожение имущества) и преднамеренные угрозы (у источника угрозы – человека есть мотив). Далее, для того, чтобы построить адекватную СОТУ безопасностью СОО, необходимо на основе проведенной идентификации ресурсов, угроз и уязвимостей определить, какой потенциально возможный ущерб ему может быть нанесен, т.е. произвести оценку риска. *Риск* – это потенциальный ущерб от реализации воздействия угроз на объект защиты. Оценка риска (ОцР) позволяет определить наиболее критичные уязвимости, наиболее актуальные для объекта угрозы, меры противодействия им, а также оптимизировать стоимостные затраты на построение системы безопасности. Итак, на данном этапе возникла триада «комплекс мероприятий по совершенствованию СОТУ – идентификация ресурсов, угроз и уязвимостей – оценка риска».

Этап 5. В результате проведенной оценки риска ОцР мы получаем как бы «карту» распределения потенциального ущерба по территории СОО. И здесь возникает проблема выбора политики управления рисками (ПолУР). Если мы выбираем принятие рисков, необходимо определить значения приемлемых рисков. В случае необходимости избегания рисков, производится поиск возможности по исключению влияния угроз на ресурсы. Чаще всего снижение уровней потенциального ущерба достигается применением соответствующих мер и средств безопасности. Определив наиболее критичные с точки зрения значений риска ресурсы СОО, мы можем сформировать состав и архитектуру комплекса организационных и технических мер обеспечения безопасности (ОиТМ). Сформировалась триада «оценка риска – политика управления рисками – комплекс организационных и технических мер обеспечения безопасности».

Этап 6. На данном этапе к комплексу ОиТМ предъявляются требования (Треб), которым конкретные средства обеспечения безопасности должны удовлетворять. Это требования конструктивного, функционального, эргономического планов. На основе предъявленных требований формируется окончательный состав комплекса технических средств безопасности (КТСБ), применение которого позволит снизить потенциальный ущерб для СОО. К текущему моменту уже становится известной архитектура КТСБ – где, какой именно тип технического средства безопасности должен быть установлен. В результате мы имеем триаду «комплекс организационных и технических мер обеспечения безопасности – требования – комплекс технических средств безопасности».

Этап 7. На предыдущем этапе была сформирована архитектура КТСБ, далее необходимо осуществить подбор конкретного оборудования, которое будет закуплено и установлено. На современном рынке средств безопасности в настоящее время сотни фирм предлагают свою продукцию покупателю. Предлагаемые средства отличаются как по своим характеристикам, так и по цене. Выбор конкретных средств безопасности, устанавливаемых на объекте, в условиях подобного разнообразия затруднен. Необходимо учесть весь спектр технических характеристик каждого элемента каждой подсистемы КТСБ, а также сравнить средства по характеристикам и цене. То есть мы приходим к задаче оценки эффективности вариантов построения КТСБ (ОцЭф). Для того чтобы сравнить варианты построения КТСБ по их эффективности, необходимо задать некоторое правило предпочтения, основанное на использовании показателей эффективности, то есть *критерий эффективности.* Конечной целью оценки эффективности КТСБ является оптимизация состава технических средств безопасности, то есть поиск наивыгоднейшего (максимального или минимального) значения критерия эффективности. При этом

следует учитывать не только эффективность совокупности технических средств, но и стоимость проектного решения. А это два показателя, находящихся в обратной зависимости друг к другу. Чем больше эффективность предлагаемого решения, тем выше будет и его стоимость, т.е. затраты на его реализацию. На основе оценки эффективности различных комплектаций КТСБ и дальнейшей оптимизации, выбирается конкретный оптимальный качественный и количественный состав организационных и технических средств обеспечения безопасности (ВС). Получилась триада «комплекс технических средств безопасности – оценка эффективности и оптимизация – выбор организационных и технических средств обеспечения безопасности».

Этап 8. Далее осуществляется заключение договоров с подрядчиками в соответствии с планом мероприятий и выделяемым финансированием, производится монтаж и ввод в эксплуатацию (МиВЭ) оборудования подсистем КТСБ, формируются необходимые регламенты, инструкции, набирается необходимый персонал. В результате всех указанных действий мы получаем реализованную систему обеспечения комплексной безопасности (СОКБ). Заключительная триада включает в себя «выбор организационных и технических средств обеспечения безопасности – монтаж и ввод в эксплуатацию – система обеспечения комплексной безопасности».

Этап 9. На заключительном этапе (этапе рефлексии) осуществляется оценка того, позволяет ли реализованная СОКБ достичь установленный целевой уровень обеспечения безопасности СОО.

Свободные концы триад можно соединять между собой, образуя новые триады. Оптимизация всего процесса достижения цели – построения эффективной СОКБ – состоит в развитии и совершенствовании каждой триады.

Концептуальная модель обеспечения безопасности. Если рассматривать методологию обеспечения безопасности как учение о системной логической организации, объектов, средств, технологий обеспечения безопасности, то ее уже можно представить в виде иерархии или следующей триады (рис. 2).

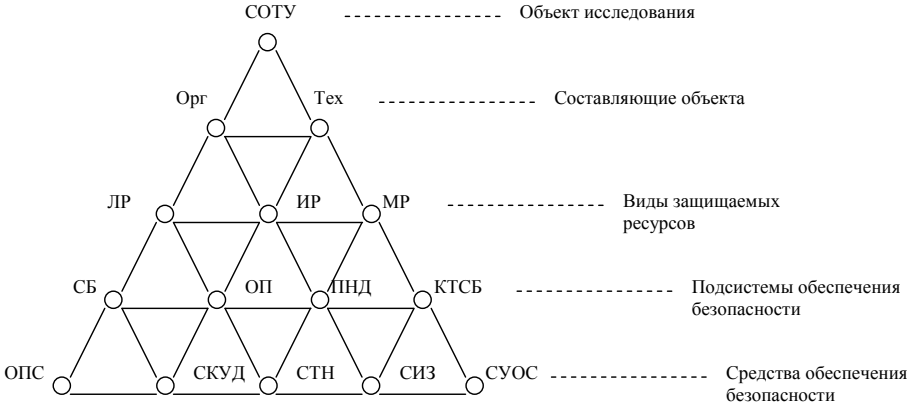

Рис. 2. Концептуальная модель обеспечения безопасности

На верхнем уровне расположена система организационно-технического управления безопасностью (СОТУ) СОО. Как уже отмечалось выше, управление безопасностью СОО имеет две взаимосвязанных составляющих: организационную (Орг) и техническую (Тех). Данный момент отражен в триаде на 2-м уровне. При разработке систем обеспечения безопасности необходимо учитывать тот факт, что СОО представляет собой совокупность ресурсов разного вида, поэтому на 3-м уровне расположены три вида ресурсов СОО, подлежащих защите: МР – матери-

альные ресурсы (оборудование, помещения, офисная техника, телекоммуникации и т.д.), ИР – информационные ресурсы (в бумажном и электронном виде), а также ЛР – людские ресурсы (персонал, посетители).

Основной целью организационно-технического управления комплексной безопасностью СОО является планирование и реализация комплекса технических средств безопасности (КТСБ), применение которого должно обеспечить состояние защищенности СОО. Данный комплекс является технической составляющей комплексной системы безопасности СОО. Что же это такое – комплексная система безопасности? Это одна из составляющих *системы обеспечения комплексной безопасности* (СОКБ) под которой понимается совокупность методов и средств поддержания безопасного состояния объекта, предотвращения, обнаружения и ликвидации угроз жизни, здоровью, среде обитания, имуществу и информации. Под совокупностью методов и средств здесь подразумеваются как органы и исполнители служб охраны и безопасности, используемые ими средства и техника, так и правовые, организационно-распорядительные и нормативные документы в области обеспечения безопасности. Таким образом, на 4-м уровне триады располагаются подсистемы СОКБ:

1. Служба охраны и безопасности (СБ);
2. Административный, операторский и технический – обеспечивающий персонал (ОП) управления системой;
3. Система правовой и нормативной документации (ПНД);
4. Комплекс технических средств безопасности (КТСБ).

Под КТСБ при этом понимается совокупность всех технических средств защиты и охраны, функциональных и интегрированных, автономных и централизованных систем, обеспечивающих безопасность и защиту объекта по установленным для него показателям и уровням защищенности.

На нижнем уровне триады располагаются средства обеспечения безопасности:

1. Охранно-пожарная сигнализация (ОПС);
2. Система контроля и управления доступом (СКУД);
3. Система телевизионного наблюдения (СТН);
4. Система инженерной защиты (заборы, стены, средства укрепленности и др.)
5. Система управления, оповещения и связи (СУОС).

Как видно из рис. 2, объект исследования (СОТУ) представляется в итоге в виде последовательного расширения триад, вложенных друг в друга и образующих единую целостную триаду в виде иерархической системы. Приведенное количество уровней не является окончательным, триаду можно расширять, дополняя различными объектами, средствами и технологиями обеспечения и управления безопасностью.

Рассмотрим, наконец, методологию обеспечения безопасности с позиций получения новых знаний на основе существующих научных подходов. Для этого сформируем иерархическую модель в виде триады, объединяющей используемые на различных этапах жизненного цикла обеспечения безопасности подходы и методы (рис. 3).

На верхнем уровне модели размещается системный подход (СП) как основополагающий элемент методологии научного познания и которым, несомненно, мы пользуемся при анализе процесса обеспечения безопасности.

Ниже расположены процессный (Проц) и проектный (Проект) подходы к решению задачи формирования системы организационно-технического управления (СОТУ) безопасностью СОО.

С точки зрения *проектного подхода* разработка СОТУ представляет собой *проект* – уникальное предприятие, предполагающее координированное выполнение взаимосвязанных действий для достижения поставленных целей в условиях ресурсных ограничений. В качестве основных признаков проекта при этом выделяют:

- уникальность и неповторимость;
- координированное выполнение взаимосвязанных действий;

- направленность на достижение конкретных целей;
- ограниченность по ресурсам, в том числе по времени (наличие начала и окончания).

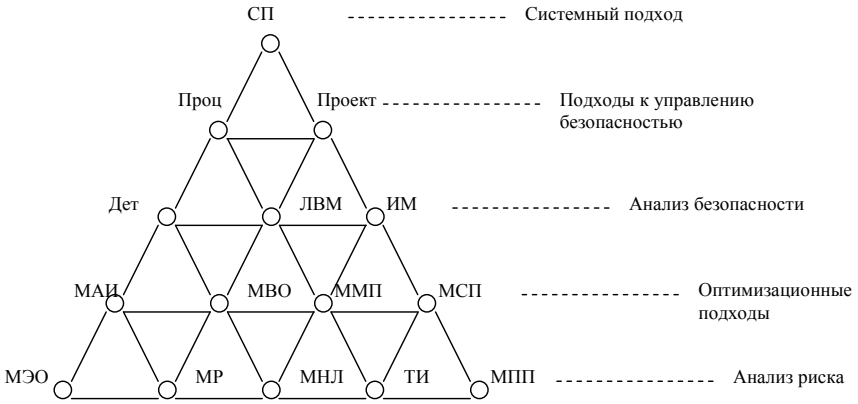

Рис. 3. Иерархическая модель научных подходов в области безопасности

Процессный подход, в свою очередь, рассматривает формирование СОТУ безопасностью как бизнес-процесс – устойчивую совокупность периодически повторяющихся действий, выполняемых для достижения определенного результата. То есть бизнес-процесс, в отличие от проекта, – это бесконечный конвейер по выполнению определенных функций. В идеале, процесс обеспечения и управления безопасностью есть нескончаемый цикл создания – оценки эффективности – корректировки – функционирования и т.д. Однако бывают ситуации и объекты, когда разработку СОТУ безопасностью целесообразно вести именно в рамках единичного проекта.

Еще ниже расположены методы анализа безопасности СОО: детерминистский подход (Дет), логико-вероятностные методы (ЛВМ), имитационное моделирование (ИМ). *Детерминистский подход* связан с заданием и последующей проверкой требований, содержащихся в нормативно-технической документации, техническом задании на проектирование, рабочем проекте оборудования объекта средствами безопасности [5]. Проводится категорирование объектов охраны в зависимости от их важности (потенциальной опасности), возможного и/или допустимого социально-экономического ущерба. Для объектов каждой категории устанавливаются дифференцированные требования по организации охраны и инженерно-технической укрепленности конструктивных элементов объекта. *Логико-вероятностные методы* позволяют получить количественную оценку риска как меры опасности. Они применяются для анализа надежности и безопасности сложных технических систем (СТС). В основе этих методов лежат два понятия: степень риска и уровень защищенности. Составляется сценарий развития опасности (граф вида «дерево»), представляющий собой логико-вероятностную модель функционирования СОО. Далее с помощью логико-вероятностных преобразований находится значение вероятностной функции P, при которой значение функции опасности равно 1 (это означает наступление опасного события), и определяется степень риска, присутствующего в системе.

Методы *имитационного моделирования* позволяют оценить различные временные параметры в системе «охрана-нарушитель». Каждая конфликтная ситуация просчитывается много раз, по результатам набирается статистика захватов нарушителя. Эффективность системы безопасности оценивается статистически как отношение числа захватов к общему числу испытаний.

Конечной целью оценки эффективности безопасности является оптимизация состава технических средств безопасности. Зачастую данная задача носит многокритериальный характер, поэтому на 3-м уровне триады (рисунок 3) представлены методы многокритериальной оптимизации структуры КТСБ:

- метод анализа иерархий Саати (МАИ);
- методы векторной оптимизации (МВО);
- методы математического программирования (ММП);
- методы стохастического поиска (МСП) оптимального значения эффективности (например, генетические алгоритмы).

Так как количество используемых характеристик элементов подсистем, число самих элементов, а также количество рассматриваемых подсистем КТСБ могут принимать довольно большие значения, в связи с чем полный перебор всех возможных вариантов построения КТСБ становится весьма трудоемким, использование методов стохастической оптимизации, а именно, генетических алгоритмов (ГА), может стать предпочтительным, поскольку применение традиционных алгоритмов многопараметрического поиска (математического программирования) в данном случае встречается с рядом трудностей.

На нижнем уровне триады располагаются методы анализа риска для ресурсов СОО: методы экспертного оценивания (МЭО), построения матрицы рисков (МР), методы, основанные на применении нечеткой логики (МНЛ), методы теории игр (ТИ), а также методы, основанные на модели системы «с полным перекрытием» (МПП). МПП представляет СОО как триаду «угрозы – средства защиты информации – объекты защиты», графически представленную в виде трехдольного графа. Достоинством данной модели является возможность анализа количественных мер уязвимости (вероятность преодоления средств защиты информации, ущерб от реализации угроз) на основе взвешивания вершин и ребер графа.

Приведенная выше триада используемых научных подходов не является «закрытой», в течение жизненного цикла СОТУ безопасностью могут применяться разнообразные подходы и методы, которые могут дополнять и расширять исходную триаду.

Выводы. Таким образом, применение триадного подхода к процессу разработки методологии обеспечения безопасности СОС позволяет системно подойти к задаче анализа жизненного цикла данного процесса, а именно, выявить последовательность триад, соединенных друг с другом и направленных на достижение конечной цели – построение эффективной СОКБ. Концептуальная модель обеспечения безопасности, построенная так же с использованием триад, в свою очередь, достаточно полно описывает иерархическую систему объектов, средств, технологий обеспечения безопасности. И, наконец, используемые на различных этапах жизненного цикла обеспечения безопасности подходы и методы также систематизированы в виде иерархической триадной модели. В целом, используя триадный подход, исследователь имеет возможность не только системно представить свои знания об исследуемом объекте, но и, расширяя и дополняя построенные триады, выявить новые свойства и закономерности, присущие объекту исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Степанов С.А., Азарьева В.В.* К качеству управления через анализ лучших практик и разработку моделей совершенства // Университетское управление: практика и анализ. – 2005. – № 5. – С. 48-55.
2. *Панюков Д.В.* Создание корпоративной концепции физической защиты объектов // Системы безопасности. – 2006. – № 2. – С. 65-67.

3. *Иванова Т.А., Строкина Ю.Г.* Система организационно-технического управления комплексной безопасностью сложного объекта (на примере вуза) // Системы управления и информационные технологии. – 2012. – №2.1 (48). – С. 203-208.
4. *Левков А.А., Ильясов Б.Г.* Триадный подход к управлению интеллектуальными информационными системами (теоретические основы) // Вестник компьютерных и информационных технологий. – 2011. – № 4. – С. 3-6.
5. *Панин О.А.* Анализ эффективности интегрированных систем безопасности: принципы, критерии, методы // Системы безопасности. – 2006. – № 2. – С. 60-62.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Васильев Владимир Иванович – ФГБОУ ВПО «УГАТУ»; e-mail: Vasilyev@ugatu.ac.ru; г. Уфа, ул. К. Маркса, 12; тел.: 83472730672; зав. кафедрой ВТиЗИ; д.т.н.; профессор.

Иванова Татьяна Александровна – e-mail: iv_tatyana@list.ru; кафедра ВТиЗИ; к.т.н.; доцент.

Ильясов Барый Галеевич – e-mail: Ilyasov@tc.ugatu.ac.ru; тел.: 83472737835; кафедра ТК; зав. кафедрой; д.т.н.; профессор.

Vasilyev Vladimir Ivanovich – USATU; e-mail: Vasilyev@ugatu.ac.ru; 12, K. Marks street, Ufa, Russia; phone: +73472730672; the department of computer science and information security; head the department; dr. of eng. sc.; professor.

Ivanova Tatyana Aleksandrovna – e-mail: iv_tatyana@list.ru; the department of computer science and information security; cand. of eng. sc.; associate professor.

Ilyasov Bariy Galeevich – e-mail: Ilyasov@tc.ugatu.ac.ru; phone: +73472737835; the department of technical cybernetics; head the department; dr. of eng. sc.; professor.

УДК 004.056

А.Ю. Гуфан, К.И. Полюшкина

КУМУЛЯТИВНЫЙ ПОДХОД К ИСПОЛЬЗОВАНИЮ ВЕРОЯТНОСТНЫХ МЕТОДОВ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается несколько типичных задач из области контроля и обеспечения информационной безопасности, традиционно решаемых с использованием методов, дающих результаты в терминах вероятности истинности предположения о том, что безопасность была нарушена. Предлагается общий подход к совместному использованию результатов анализа нескольких объектов, относящихся к информационной системе, либо процессов, происходящих в ней, либо нескольких характеристик таких объектов или процессов. Показано, что интерпретация такой совокупности результатов анализа может дать более точную информацию о состоянии системы, чем простая дизъюнкция отдельных результатов, получаемых при анализе каждого объекта или процесса, или их характеристик по отдельности. Рассмотрены примеры задач стеганографического анализа, выявления вредоносных вложений в файлах неисполнимых форматов, поиска аномалий поведения пользователей информационных систем. Для каждой из этих задач выявлены особенности, критически влияющие на возможность и специфику применения к ним предлагаемого подхода и предложены пути преодоления связанных с этими особенностями проблем.

Аномалии поведения пользователей; нейронные сети; стеганографический анализ.