УДК 004.056

КОНФЛИКТНО-АКТИВНОЕ УПРАВЛЕНИЕ ПРОЕКТАМИ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

© 2022 К. А. Плющик, Д. Е. Орлова

Воронежский институт ФСИН России (Воронеж, Россия)

Разрабатывается концепция конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей. В соответствие с этой концепцией управление проектами данного типа рассматриваться как процесс разрешения антагонистического конфликта между системой обеспечения безопасности инфокоммуникационных сетей и злоумышленниками (преступными элементами), осуществляющими деструктивные воздействия на компоненты этих сетей.

Ключевые слова: инфокоммуникационная сеть, управление, проект, конфликт, рефлексия.

Введение. В условиях тотальной компьютеризации и цифровизации современного общества инфокоммуникационные сети все в большей мере становятся подверженными деструктивным воздействиям. В этом аспекте следует особо подчеркнуть, что злоумышленники и преступные элементы постоянно совершенствуют приемы, методы и средства деструктивных воздействий на компоненты инфокоммуникационных сетей. В результате процесс их проектирования, разработки и эксплуатации непременно сопровождается антагонистическими конфликтами между системой обеспечения информационной безопасности и системой «разрушения» этой безопасности, негативный исход которых может привести к невосполнимым потерям.

Общетеоретическим вопросам разработки и совершенствованию методов и средств защиты информации, а также обеспечению информационной безопасности различных объектов от внешних и внутренних угроз хищения, разрушения и/или модификации информации, посвящено значительное число научных работ как у нас в стране, так и за рубежом. В целом следует заключить, что проблема информационной безопасности находится в центре внимания ученых и практиков, и при ее решении достигнуты крупные результаты, позволяющие утверждать о существовании научного и практического задела в этой области.

Вместе с тем, при наличии значительного научного задела в сфере информационной безопасности, проблема управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей оказалась вне поля научных изысканий и пока не получила должного решения. Как показывает анализ, в настоящее время сущностная сторона управления проектами этого класса сводится к разработке, так называемой, модели угроз, передачи ее разработчикам защищаемых объектов и осуществления контроля выполнения требований этой модели при принятии проектных решений [1, 2]. Это означает, что фактически управление проектами развития систем обеспечения информационной безопасности отдано на откуп разработчикам или лицам, обеспечивающим функционирование защищаемых инфокоммуникационных сетей, и рассматривается скорее, как плановая проверка соблюдения нормативных требований, чем наука, базирующаяся на последних достижениях в области управления проектами. Фактически проекты по обеспечению безопасности встраиваются в проекты по развитию инфокоммуникационных сетей, занимая в них, хотя и важное, но, все же второстепенное место. В результате происходит потеря системности целостности проекта: проблемы информационной безопасности ре-

Плющик Кирилл Александрович – Воронежский институт ФСИН России, адъюнкт, e-mail: victor_novo@mail.ru.
Орлова Дарья Евгеньевна – Воронежский институт ФСИН России, кандидат технических наук, преподаватель.

шаются путем использования отдельных антивирусных программ и сетевых экранов, без полноценного управления всем процессом управления безопасностью [10].

Последствия такого подхода, вылились еще и в то, что к настоящему времени не создана система проблемно-ориентированных математических моделей поддержки принятия решений в ходе управления проектами рассматриваемого типа. В результате деятельность специалистов и должностных лиц, осуществляющих управление процессами обеспечения информационной безопасности, оказалась не поддержанной ни методологическим, ни математическим аппаратом. Проектные решения, как и ранее, им приходится принимать на свой страх и риск, опираясь на личный опыт, логику здравого смысла и интуицию, или приспосабливая для своих нужд ранее разработанные модели, ориентированные на другие задачи.

Учитывая сказанное, можно утверждать, что проблема управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей актуальна и ее решение имеет непосредственное практическое значение.

Исходные положения. При решении этой проблемы будем учитывать следующие факторы, характерные для процесса управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей [8]:

- сложность и конфликтность предметной области (достаточно большое количество разнообразных функций, объектов, атрибутов и разнообразие взаимосвязей между ними), требующими при управлении проектами комплексного анализа и учета этих обстоятельств;

- наличие тесно взаимодействующих разнородных типов управленческих решений, имеющих свои локальные критерии, зачастую входящие в противоречие друг с другом, что порождает необходимость их согласования и координации;

- отсутствие прямых аналогов, что существенно ограничивает возможность использования (прямого заимствования) каких-либо типовых управленческих решений и моделей для поддержки принятия этих решений;

- разобщенность и разнородность коллективов разработчиков как по уровню квалификации, так и по сложившимся традициям использования тех или иных инструментально-программных средств;

Если говорить о методологических факторах, оказывающих влияние на управление рассматриваемыми проектами, то необходимо указать следующее [9]:

- субъективный не всегда формализуемый характер целей управления и критериев принятия управленческих решений, обусловленный наличием людей в узлах управления, обладающих определенной свободой в выборе своего поведения и своими собственными интересами, не всегда совпадающими с интересами заказчика и руководителя проекта;

- многокритериальный и взаимозависимый характер целей и критериев принятия управленческих решений, обусловленный тем, что объект управления характеризуется множеством различных по своей сути аспектов социального, экономического, технического, технологического и организационного свойства, часть из которых в силу ряда причин оказываются противоречивыми и изменяющимися во времени;

- неопределенный характер исходных данных, используемых, лицами, осуществляющими управление рассматриваемыми проектами, вероятностного, структурного, лингвистического и иного свойства;

- неполностью формализуемый характер параметров объекта управления и его среды, обусловленный тем, что многие его сущностные свойства и связи с окружающими объектами не настолько хорошо и полно выяснены, чтобы их можно было выразить в числах и измерять на количественных шкалах.

Естественно, что отмеченные факторы в существенной мере усложняют управление проектами данного типа, не позволяя свести его к решению, например, оптимизационной математической задачи (пусть сколь угодно сложной). Однако это скорее техническая сторона дела. Важнейшим фактором, предопределяющим концепцию управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей, является фактор конфликтности между проектируемой системой обеспечения безопасности и системой «раз-

рушения» (преодоления) этой безопасности. Традиционно этот фактор непременно учитывается при проектировании систем защиты информации, однако напрямую не предопределяет структуру управления проектами развития систем этого класса и идеологию разработки математического аппарата поддержки принятия управленческих решений в части управления безопасностью. В итоге имеем пассивную сущность существующего подхода к управлению проектами рассматриваемого типа, когда все усилия разработчиков направлены исключительно на защиту информации, циркулирующей в инфокоммуникационных сетях, а вопросы активного воздействия со стороной, стремящейся преодолеть барьеры безопасности, остаются вне поля зрения проектировщиков. В условиях постоянно растущей эффективности деструктивных воздействий, оказываемых злоумышленниками и преступными элементами, как на компоненты инфокоммуникационных сетей, так и на саму систему их защиты, такую концепцию нельзя признать конструктивной.

Суть конфликтно-активной концепции. Управление проектами данного типа должно рассматриваться как процесс разрешения антагонистического конфликта между системой, осуществлявшей управление проектами, и системой, планирующей осуществлять деструктивные воздействия на объект управления – защищаемую инфокоммуникационную сеть, с целью обеспечения безусловного превосходства над злоумышленниками и преступными элементами, организующими и реализующими эти воздействия. При этом исполнители проектов выступают не пассивной стороной, а представляют собой активную систему, которая не только возводит барьеры безопасности, но и воздействует на элементы, пытающиеся преодолеть эти барьеры. Схема такой концепции показана на рисунке 1.

Как видно из этой схемы, процесс управления проектами развития систем этого класса связан с необходимостью разрешения конфликтов трех типов.

Первый тип конфликтов можно условно назвать *опосредованными*. В них участвуют, с одной стороны, разработчики, проектировщики и персонал защищаемых инфокоммуникационных сетей, а, с другой стороны, злоумышленники и преступные элементы, осуществляющие деструктивные воздействия на эти сети. Второй тип конфликтов, можно условно назвать *непосредственными*. Их участниками, с одной стороны, являются лица, ответственные за управление проектами обеспечения информационной безопасности инфокоммуникационных сетей, их разработчики, проектировщики и персонал, а, с другой стороны – те же злоумышленники и преступные элементы, осуществляющие деструктивные воздействия на эти сети.

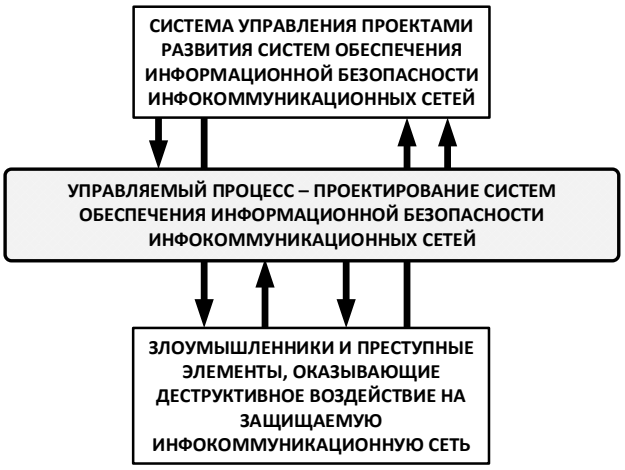

Рисунок 1. Схема конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей

Третий тип конфликтов условно можно назвать *прямыми*. В этих конфликтах, названные выше стороны применяют уже не организационно-технические способы и средства борьбы, а осуществляют приемы и методы информационного и иного воздействия непосредственно друг на друга, реализуя активный рефлексивный подход к управлению сложными организационно-техническими системами.

В целом предлагаемая схема, по сути, отражает процесс поиска рациональных проектных решений в условиях трехуровневого конфликта между системой обеспечения безопасности и системой «разрушения» этой безопасности, при соблюдении объективно существующих ограничений экономического, производственного, технологического, организационного и временного плана.

Способы реализации конфликтно-активной концепции. Для реализации рас-

смотренной схемы конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей предлагается использовать рефлексивный подход [3-7], суть которого применительно к нашему случаю заключается в следующем. Если при обычном управлении проектами рассматриваемого типа речь идет о компенсации внешних отклоняющих воздействий, учете влияния внешней среды и прогнозировании вероятных деструктивных воздействий со стороны злоумышленников и преступных элементов, то при рефлексивном подходе сторона, осуществляющая управление, стремиться к тому, чтобы заставить (принудить) злоумышленников и преступных элементов действовать так, как это выгодно ей самой. Для этого на каждом этапе управления она должна:

- установить потребности и интересы злоумышленников и преступных элементов, то есть понять мотивы, определяющие их решения и поступки, выявить стратегию и тактику применения средств деструктивных воздействий и их возможности;

- определить (обычно путем проведения специальных мероприятий) возможные варианты действий злоумышленников и преступных элементов, способы возможных действий, ресурсные и коммуникационные возможности, а также уровень оснащения средствами, способными осуществлять деструктивные воздействия на компоненты защищаемой инфокоммуникационной сети, построить, так называемую, модель угроз при тесном взаимодействии с подразделениями «К» МВД России;

- принять (опираясь на эти данные) решение относительно возможных вариантов собственного поведения и на этой основе рассчитать выгодную для себя стратегию поведения злоумышленников и преступных элементов;

- изыскать способы и передать противнику (также путем проведения специальных операций) такие данные об объекте защиты, а также о своих намерениях и планах действия, которые побудят злоумышленников и преступных элементов выбрать стратегию и тактику своего поведения, выгодную для лиц, осуществляющих управление проектами защиты.

Отметим основные свойства рефлексивного управления, которые должны учитывать лица, осуществляющие управление проектами рассматриваемого типа, в своей практической деятельности.

Рефлексивное управление носит взаимно отражательный характер («А» думает, что «В» предполагает, что «А» примет решение, рассчитывая на то, что «В» ответит и т. д.) с соответствующими рангами рефлексии каждого участника конфликта, определяемые следующим образом:

- сторона «А» обладает нулевым рангом рефлексии ($RR^A = 0$), если она в своем поведении руководствуется гарантированными (максиминными) стратегиями, то есть выбирает из всех возможных вариантов поведения противника наихудший для себя вариант и применительно к нему ведет себя наилучшим образом: в том случае, когда сторона «А» строит свое поведение, предполагая, что противник имеет нулевой ранг рефлексии ($RR^B = 0$), она обладает первым рангом рефлексии ($RR^A = 1$); второй ранг рефлексии ($RR^A = 2$) имеет тесто в том случае, когда сторона «А» предполагает, что ее противник обладает первым рангом рефлексии ($RR^B = 1$); сторона «А» обладает K-м рангом рефлексии, если она предполагает, что ее противник имеет $(K - 1)$-й ранг рефлексии. Формула для определения ранга рефлексии выгладит так: $(RR^B = K - 1) \rightarrow (RR^A = K)$, Превосходство в ранге рефлексии обеспечивает при прочих равных условиях преимущество, поскольку сторона с более высоким рангом рефлексии, переигрывает противника, навязывая ему свою линию поведения.

При рефлексивном управлении особую значимость приобретает использование «умной дезинформации» совместно с комплексным противодействием разведке противника. Это осуществляется, например, показом ему ложных признаков каких-либо объектов, передачей ему специально мотивированной информации, силовым подавлением его источников информации, защитой собственных информационных каналов от утечки. Эти и другие мероприятия должны быть рассчитаны на то, что злоумышленники и преступные элементы примут неверное, несоответствующее ситуации решение о типах, характеристиках или возможностях увиденных объектов и о способах борьбы с ними. Обязательным условием дезинформа-

ции является и достаточная правдоподобность, обеспечивающая преодоление «фильтров», которые помогают противнику выделять полезную и реальную информацию из общей массы собираемой (поступающей).

Обоюдная реализация рефлексивного управления создает неопределенность в принятии управленческих решений у обеих сторон. В условиях взаимной рефлексии невозможно однозначно предсказать «что будет дальше», а можно лишь спрогнозировать «что может произойти потом, если мы сейчас делаем нечто». Это приводит к тому, что при практической реализации рефлексивного подхода при управлении проектами становится бессмысленной и даже опасной традиционная постановка вопроса «что делать?», и предпочтение следует отдать другому вопросу – «чего не следует делать и чего следует опасаться?». Естественно, что в такой постановке вопроса также содержится неопределенность, но она уже меньшего порядка, чем исходная неопределенность. В первом же случае, когда лица, осуществляющие управление проектами, пытаются ответить на вопрос «что делать?», неопределенность не уменьшается, а лишь создается иллюзия однозначности и определенности.

Немаловажным свойством рефлексивного управления является его динамичность. Рефлексия становится эффективной только тогда, когда каждый ее шаг сопровождается вариациями в способах мотивации противника. При этом для лиц, осуществляющих управление проектами с использованием рефлексивного подхода, важно не только отслеживать поведение злоумышленников и преступных элементов и реагировать на их действия, но и упреждать их намерения, периодически вводя в заблуждение относительно собственных намерений.

Рассмотрим способы реализации рефлексивного управления.

Рефлексия посредством формирования ложной картины. Это один из наиболее распространенных способов рефлексии, предполагающий, дать злоумышленникам и преступным элементам вполне определенные, но заведомо ложные данные, о применяемых и планируемых к применению средствах защиты информации, и перспективах их развития, а не ликвидировать вообще поступление любой информации.

Рефлексия посредством формирования цели противника, реализуемая, например, в форме рекламы фантомных (несуществующих) средств защиты информации или раскрытия ложных планов проведения опытно-конструкторских работ.

Рефлексия посредством формирования доктрины противника. Например, злоумышленникам регулярно внушаются типовые приемы и способы информационной защиты. В результате у них закрепляется данная информация как стандарт, что и используется для достижения успеха в решающий момент.

Рефлексия посредством демонстрации ложных намерений. Осуществляется сознательным сбросом соответствующей документации. Кроме того, рефлексией такого типа будет «подтверждение» того, что замаскированные объекты противника не вскрыты (хотя на самом деле они вскрыты), а «ложные объекты», построенные противником, восприняты как «настоящие объекты», хотя на самом деле их ложность установлена.

Рефлексия путем создания у противника ложных представлений о своем состоянии. Сущность этого способа заключается в том, чтобы информационными действиями сформировать у злоумышленников и преступных элементов завышенную или заниженную оценку собственных возможностей по оказанию деструктивных воздействий на объект защиты. В принципе это возможно, поскольку любая оценка относительна и субъективна. Следовательно, речь идет о том, чтобы представить злоумышленникам и преступным элементам такую (внешне объективную) информацию, основываясь на которой они либо недооценят, либо переоценят собственные возможности. Как в том, так и в другом случае, принимаемые ими действия будут неадекватными.

Выше были рассмотрены, так называемые, простые способы рефлексии. Вместе с тем существуют и сложные (более глубокие) способы рефлексивного воздействия на злоумышленников и преступных элементов [3]. Различие этих способов состоит в том, что, если простые способы сводятся к воздействию только на процесс отображения обстановки (ситуации) у этих субъектов, то сложные способы сводятся к воздействию на сам процесс принятия решений противосто-

ящей стороны, то есть к управлению самой рефлексией. Рассмотрим содержание этих способов.

В зависимости от объекта приложения эти способы можно разделить на две группы: прямого и опосредованного влияния на процесс принятия управленческих решений злоумышленниками и преступными элементами. Прямое воздействие реализовывается целенаправленным информационно-психологическим влиянием на компоненты принятия решений этими субъектами. Схема этих воздействий показана на рисунке 2.

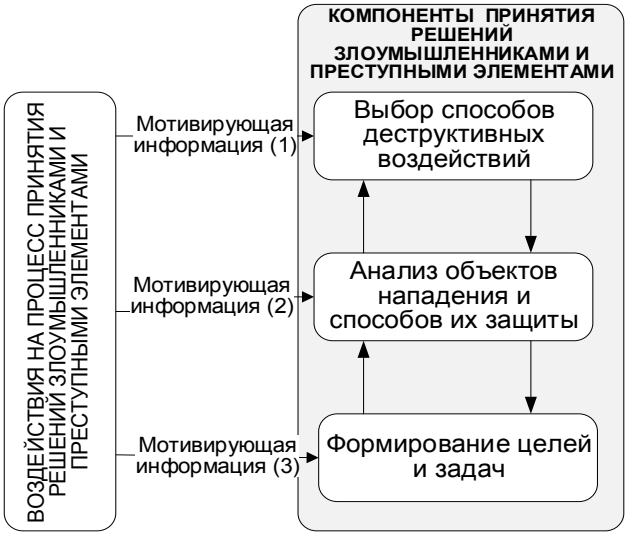

Рисунок 2. Схема прямого воздействия на процесс принятия решения злоумышленниками и преступными элементами

В результате таких воздействий у злоумышленников и преступных элементов возникают проблемы следующего свойства:

- сужается круг альтернативных вариантов организации деструктивных воздействий на защищаемые инфокоммуникационные сети, либо из числа альтернатив исключаются наиболее важные (с точки зрения эффективности) варианты решений;
- происходит дезориентация относительно условий применения средств воздействия на инфокоммуникационные сети и результатов их применения;
- нарушается логика выбора способов деструктивных воздействий так, что эти способы оказываются выгодными не им, а стороне, обеспечивающей защиту инфокоммуникационных сетей.

Еще более значительный эффект получается при опосредованном информационно-психологическом влиянии на процесс принятия решений злоумышленниками и преступными элементами, путем воздействия не на сами решения, а на те факторы, которые определяют и обусловливают выработку ими решений. К таким факторам относятся: понятия, которыми оперируют злоумышленники и преступные элементы в своей деятельности; критерии, которыми они руководствуется при принятии решений; ограничения, социального, морального, правового и иного плана, которые они учитывают при совершении своих поступков. Схема этих воздействий показана на рисунке 3.

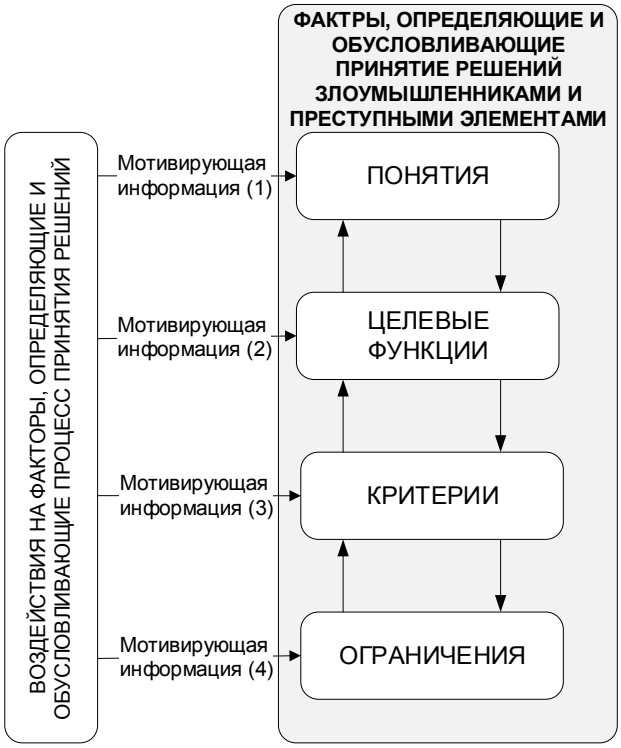

Рисунок 3. Схема опосредованного воздействия на процесс принятия решения злоумышленниками и преступными элементами

При формировании этой схемы учитывался тот факт, что многие субъекты, которые именуются злоумышленниками и преступными элементами, не являются закоренелыми нарушителями законов, а оказались втянутыми в противоправный процесс в силу своей неправильной и неустойчивой социальной ориентации. В этом случае возможными результатами реализации предложенной схемы могут быть:

- формирование у лиц, втянутых в преступный процесс, правильно ориентированной системы понятий;

- корректировка их целевых функций, на которые они ориентируются в своей повседневной деятельности;

- переориентирование в правильном направлении критериев принятия решений, которыми они оперируют в своей жизни;

- расширение и правильное понимание ими существующих социальных, правовых, культурных и иных норм.

В целом результаты проведенных исследований позволяют заключить, что существует достаточно большое разнообразие способов практической реализации рефлексивного подхода при конфликтно-активном управлении проектами развития систем обеспечения информационной безопасности критически важных объектов социально-экономической инфраструктуры. Если попытаться провести их ранжирование с точки зрения эффективности практического применения, то следует констатировать, что наиболее действенными в этом смысле являются способы, реализующие сложное рефлексивное воздействие. Вместе с тем, если учитывать системный характер обработки информации субъектами, на которых направлены эти воздействия, то наиболее целесообразным следует признать комплексную реализацию воздействий, сочетающую все рассмотренные выше способы. При этом следует варьировать эти способы так, чтобы злоумышленники и преступные элементы не успевали адаптироваться к изменяющимся условиям рефлексии.

При практической реализации указанных выше способов рефлексии необходимо учитывать, что в арсенале злоумышленников и преступных элементов имеется свой набор способов оказания информационно-психологических воздействий как на лиц, осуществляющий управление рассматриваемыми проектами, так и на персонал защищаемых инфокоммуникационных сетей. Эти способы они, как правило, заимствуют из арсенала способов, так называемого «психологического террора», а именно:

- угрозы физического нападения на сотрудников предприятий, участвующих в проектировании и разработки средств защиты, а иногда и на членов их семей;

- угрозы повреждения, принадлежащего им имущества;

- аргументированное воздействие на психику сотрудников для снятия морально-этических и социальных барьеров;

- обещания материального вознаграждения за выполненные поручения противоправного плана;

- вовлечение в антисоциальные и преступные группы;

- понижение социального статуса и значимости сотрудников в коллективе, когда занижаются их положительные качества, их опыт и уровень квалификации;

- прямой и косвенный шантаж сотрудников с учетом их прошлых правонарушений и упущений в работе;

- предварительное применение психотропных и других биологически активных веществ, оказывающих влияние на психические функции человека (в том числе на эмоции и поведение) и способных переводить его в измененное состояние сознания;

- «программирование» мотивов, жизненных установок, стереотипов, устремлений, настроений и даже психического состояния сотрудников с целью обеспечения такого их поведения, которое нужно злоумышленникам и преступным элементам.

При этом можно выделить следующие этапы, которые реализуют злоумышленники и преступные элементы, планируя и организуя мероприятия по оказанию информационно-психологического давления на персонал предприятий, участвующий в проектировании и разработки средств защиты инфокоммуникационных сетей: определение целей и вероятных объектов информационно-психологического воздействия; сбор информации о наиболее подходящих объектах информационно-психологического воздействия и анализ их психофизиологических данных; выбор наиболее подходящих способов и приемов оказания информационно-психологического давления; реализация этих способов путем передачи соответствующей информации выбранным объектам воздействия и контроль реакции объекта на воздействие.

Структурная модель конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей. С учетом отмеченных особенностей,

структурная модель управления проектами рассматриваемого типа может быть представлена в виде кортежа:

$$\langle\langle US_1, US_2\rangle, \langle UO\rangle, \langle V_1, O_1\rangle, \langle V_2, O_2\rangle, \langle p_{pu}^{(1)(2)}, p_{os}^{(1)(2)}, p_{up}^{1}, r^{(1)(2)}\rangle, \langle p_{pu}^{(2)(1)}, p_{os}^{(2)(1)}, p_{up}^{2}, r^{(2)(1)}\rangle, \langle p_{uu}^{1}, p_{uu}^{2}\rangle, \langle \langle \xi_{kr}, \xi_f\rangle\rangle,$$

где US_1 – команда проекта (проектировщики), US_2 – злоумышленники и преступные элементы; UO – процесс проектирования системы обеспечения информационной безопасности инфокоммуникационных сетей; . u_1 – канал прямого управления процессом со стороны проектировщиков, u_2 – канал прямого управления процессом со стороны злоумышленников и преступных элементов, O_1, O_2 – каналы обратной связи; $p_{pu}^{(1)(2)}$, $p_{pu}^{(2)(1)}$ – взаимные воздействия проектировщиков и злоумышленников на каналы прямого управления; $p_{os}^{(1)(2)}$, $p_{os}^{(2)(1)}$ – взаимные воздействия проектировщиков и злоумышленников на каналы обратной связи; $p_{up}^{(1)(2)}$, $p_{up}^{(2)(1)}$ – непосредственные воздействия управляющих субъектов друг на друга; $r^{(1)(2)}$, $r^{(2)(1)}$ – взаимная разведка намерений и действий противостоящих сторон; p_{uu}^{1}, p_{uu}^{2} – воздействия управляющих субъектов самих на себя с целью повышения качества своего управления; ξ_{kr} – внешние целевые возмущения, стремящиеся перевести управляемый процесс в то или иное состояние; ξ_f – внешние фоновые возмущения, то есть внешние воздействия не имеющие целевой направленности, но влияющие на развитие управляемого процесса.

В схематическом изображении структурная модель конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей представлена на рисунке 4.

Заметим, что воздействия сторон друг на друга могут быть как физическими, так и информационными. Так, например, воздействия $p_{up}^{(1)(2)}$ и $p_{up}^{(2)(1)}$ могут осуществляться как в форме физического устранения у противника информационно значимых субъектов, так и путем их дезинформации. Воздействия p_{uu}^{1} и p_{uu}^{2} могут осуществляться в форме сокращения численности управленческого персонала, изменения функциональных обязанностей и других организационно-штатных мероприятий, способствующих повышению качества управления. Вместе с тем, не исключены случаи, когда воздействия p_{uu}^{1} и p_{uu}^{2} направляются в другую сторону: это ситуации преднамеренного разрушения (ликвидации) противника.

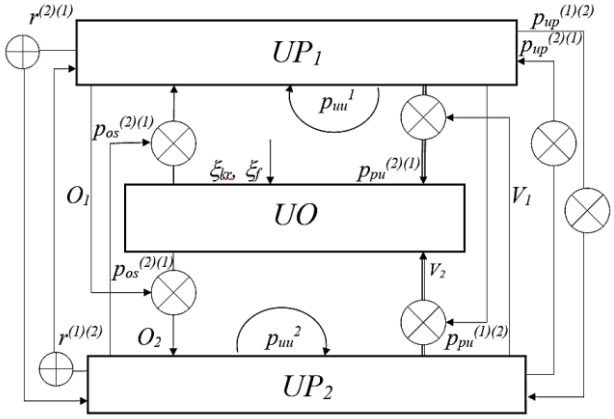

Рисунок 4. Структурная модель конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей

Из этой модели становится очевидным, что существующая модель управления рассматриваемыми проектами является частным случаем конфликтно-активного управления. Действительно, если исключить из схемы рис. 4 злоумышленников и преступные элементы (US_2), то приходим к существующей модели управления проектами данного типа.

Заключение. Изложенная в статье концепция управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей привносит существенно важные компоненты в управление этим процессом. В отличие от традиционной бесконфликтной схемы, управление проектами данного типа предлагается рассматривать как поэтапный циклический процесс поиска рациональных проектных решений в условиях конфликта между системой обеспечения безопасности и системой «разрушения» этой безопасности, в котором исполнители проектов выступают не пассивной стороной, а представляют собой активную систему. Это позволяет более адекватно и целенаправленно учесть фактор постоянно растущей эффективности деструктивных воздействий, оказываемых злоумышленниками и преступными элемен-

тами как на компоненты защищаемых инфокоммуникационных сетей, так и на саму систему их защиты.

СПИСОК ИСТОЧНИКОВ

1. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: Моск. гос. инж.-физ. ин-т (техн. ун-т). 1997. – 537 с.

2. Кочедыков С. С. Тензорный анализ Крона и его приложения / В. И. Новосельцев, Д. Е. Орлова, С.С. Кочедыков; под ред. В.И. Новосельцева. – Воронеж: Научная книга, 2017. – 260 с.

3. Кочедыков С. С. Типология взаимного влияния программных компонентов информационных систем в условиях внешних и внутренних угроз / С. С. Кочедыков, А. С. Кравченко, В. И. Новосельцев // Вестник Воронежского института ФСИН России. 2017. – № 2. – С. 77-84.

4. Львович Я. Е. Оптимизация проектирования многоаспектной цифровой среды системы однородных объектов на основе процедур декомпозиции и агрегации / Я. Е. Львович, А. В. Питолин, С. О. Сорокин // Моделирование, оптимизация и информационные технологии. – 2019. – Т. 7. – № 2 (25). – С. 186-195.

5. Модели управления конфликтами и рисками / С. А. Баркалов [и др.]; Под ред. Д. А. Новикова. – Воронеж: Научная книга, 2008. – 470 с.

6. Новосельцев В. И. Системная теория конфликта / В. И. Новосельцев Б. В. Тарасов. – М: Майор, 2011. – 336 с.

7. Плющик К.А. Состояние системы информационной безопасности в российских ведомствах, отвечающих за общественную безопасность и правопорядок. Вестник Воронежского института ФСИН России. – 2021. – № 2. – С. 82-87.

8. Риск и рефлексия / Под ред. В.И. Новосельцева. – М.: Горячая линия – Телеком, 2016. – 146 с.

9. Теоретические основы управления в системах организационного поведения / Под общей ред. В.И. Новосельцева. – Воронеж: ИПЦ «Научная книга». 2021. – 380 с.

10. Управление конфликтами: учебное пособие для вузов / В. П. Балан [и др.]; Под ред. В. И. Новосельцева. – М.: Горячая линия – Телеком, 2015. – 144 с.

11. Язов Ю. К. Основы технологии проектирования систем защиты информации в телекоммуникационных системах: учебное пособие / Ю. К. Язов. – Воронеж: Воронеж. гос. техн. ун-т, 2005. – 318 с.

CONFLICT-ACTIVE PROJECT MANAGEMENT FOR THE DEVELOPMENT OF INFORMATION SECURITY SYSTEMS FOR INFOCOMMUNICATION NETWORKS

© 2022 K. A. Plushik, D. E. Orlova

Voronezh Institute of the Federal Penitentiary Service of Russia (Voronezh, Russia)

The concept of conflict-active project management for the development of information security systems of infocommunication networks is being developed. In accordance with this concept, the management of projects of this type is considered as a process of resolving an antagonistic conflict between the security system of infocommunication networks and intruders (malicious elements) carrying out destructive effects on the components of these networks.

Keywords: infocommunication network, management, project, conflict, reflection.