УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

***Калашников Андрей Олегович**, доктор технических наук*

В работе рассматриваются проблемы эффективного управления информационными рисками объектов критической информационной инфраструктуры Российской Федерации с использованием моделей и методов теории управления организационными системами. Проведен анализ моделей информационных угроз и рисков для организационных систем с различными структурами и свойствами. Показано, что предлагаемый для управления информационными рисками набор, состоящий из механизмов мотивационного, институционального и информационного управления, является полным в том смысле, что целиком покрывает, как множество классов потенциально возможных информационных угроз, так и множество всех типов контрмер. При этом набор механизмов мотивационного управления для управления информационными рисками организационных систем, включающий механизмы планирования (распределения ресурса), стимулирования и страхования, является необходимым и минимально достаточным.

***Ключевые слова**: информационный риск, организационная система, организационное управление*

INFORMATION RISK MANAGEMENT OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

***Andrey Kalashnikov**, Doctor of Technical Sciences*

In this paper we consider the problem of effective information risk management objects of the critical information infrastructure of the Russian, using models and methods of the theory of organizational systems control. The analysis models of information threats and risks to organizational systems with different structures and properties. It is shown that the proposed management information risk set consisting of motivational mechanisms, institutional and information management, is complete in the sense that it completely covers as many classes of potential information threats and the set of all types of countermeasures. In this case, a set of mechanisms for motivational mechanisms of information risk management organizational systems, including planning tools (resource allocation), incentives and insurance is a necessary and sufficient minimum

***Keywords**: information risk, organizational system, organizational management*

1. Введение

Современный этап развития России характеризуется переходом на новый, более интенсивный путь развития, который затрагивает все сферы жизнедеятельности государства и общества: экономики и финансов, промышленности и энергетики, транспорта и связи, обороны и безопасности, науки и культуры, образования и здравоохранения, государственного управления и многих других. В этом процессе можно выделить ряд характерных особенностей, на две из которых необходимо обратить особое внимание. Это, во-первых, значительное повышение требований к качеству и эффективности управления, а, во-вторых, интенсивное внедрение и использование передовых *информационных технологий*[1] (ИТ) во всех указанных выше сферах.

Однако широкое и повсеместное использование ИТ в различных организациях имеет свою «оборотную сторону», проявляющуюся в том, что

1 *Информационная технология* – приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных ([1], ст. 3.1.9).

успешная компьютерная атака на одну из таких организаций может привести не только к нарушение или прекращение ее функционирования, но и к более глобальным последствиям в виде потери управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени. Такие организации, в соответствии с проектом Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[2] относятся к *критически важным объектам* (далее, КВО). Совокупность информационных технологий и систем КВО, а также обеспечивающих их взаимодействие информационно-телекоммуникационных сетей и информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка образуют критическую информационную инфраструктуру Российской Федерации (далее, КИИ РФ)[3].

Возможность нарушения безопасности ИТ порождает риски, которые с этими технологиями связаны – *информационные риски*[4], которые, представляют собой отрицательные последствия целенаправленного и/или случайного воздействия на объекты КИИ РФ, выразившиеся в утечке, хищении, утрате, подделке, искажении и несанкционированном доступе к информации, а также в отклонении от установленных эксплуатационных пределов и условий функционирования объектов КИИ РФ. В свою очередь, наличие информационных рисков с неизбежностью приводит к необходимости поиска эффективных методов *управления*[5] ими.

2. Постановка задачи

С точки зрения теории управления любое предприятие, учреждение, корпорация, входящие в состав объектов критической информационной инфраструктуры Российской Федерации, представляет собой *организационную систему*[6] (ОС), имеющую определенные цели и решающую определенные задачи, а управление указанной ОС – вид деятельности субъекта управления, направленный на перевод системы из текущего состояния в желаемое.

Рассмотрим базовую модель ОС, в состав которой входят: управляющий субъект (далее, *центр*), управляемый субъект (далее, *агент*), объект управления и внешняя среда (*природа*).

В рамках принятой модели управления ОС центр осуществляет воздействие на агента, который, в свою очередь, воздействует на объект управления.

Предположим, далее, что задан *критерий эффективности* функционирования ОС, зависящий от *управляющего воздействия* центра, действия агента и *состояния* внешней среды. Тогда, исходя из *гипотезы рационального поведения*, можно предположить, что центр, с учетом всей имеющейся у него информации, будет выбирать такие управляющие воздействия, которые будут максимизировать критерий эффективности.

Если ОС функционирует в условиях полной информированности центра обо всех существенных внешних и внутренних по отношению к системе параметрах, включая состояние внешней среды и действий агента (*детерминированная* ОС), то решение задачи нахождения «*эффективного управления*» носит скорее «технический» характер.

Перейдем теперь к рассмотрению задачи управления ОС в условиях неопределенности, то есть, когда имеется необходимость принимать решение в ситуации, известной не полностью. Основная трудность при этом состоит в том, что последствия, связанные с принятием того или иного решения, зависят от неизвестной ситуации или параметров, что отрицательно сказывается на эффективности управления. Иными словами, наличие в управляемой системе того или иного вида неопределенности создает потенциальную возможность не достижения цели управления – максимизации критерия эффективности.

---

2 http://regulation.gov.ru/project/5890.html?point=view_project&stage=2&stage_id=2938

3 Там же.

4 *Риск* – влияние неопределенностей на процесс достижения поставленных целей. Примечания: 1) цели могут иметь различные аспекты: финансовые, связанные со здоровьем, безопасностью и внешней средой и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса; 2) риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а так же на то, как они могут влиять на достижение целей; 3) риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности ([1], ст. 3.2.9).

5 *Управление рисками* – координированные действия по направлению и контролю над деятельностью организации в связи с рисками ([1], ст. 3.2.16).

6 *Организационная система* (organization) – объединение людей (например, корпорация, предприятие, объединение, фирма), совместно реализующих некоторую программу или цель и действующих на основе определенных процедур и правил (механизмов) ([2]).

3. Анализ задачи

При рассмотрении математических моделей принятия решений необходимо принимать во внимание наличие в них следующих видов неопределенности: *объективную неопределенность* и *субъективную неопределенность*, которые могут иметь место либо относительно параметров, описывающих компоненты организационной системы (*внутренняя неопределенность*), либо относительно внешних параметров (*внешняя неопределенность*) (см. подробнее [2]).

В свою очередь, при рассмотрении информационных угроз, направленных на информационно-технологическую инфраструктуру объектов КИИ РФ, как правило, выделяют следующие их классы (см., например, [1], ст. 3.1.2): *естественные*, подразделяющиеся на *природные* и *техногенные*, и *искусственные* (антропогенные), подразделяющиеся на *случайные* и *преднамеренные*. Также информационные угрозы могут быть классифицированы по месту своего возникновения, как *внутренние* и *внешние* по отношению к рассматриваемой системе. Между имеющимися в ОС неопределенностями управления и информационными угрозами существует очевидное соответствие. Иными словами, наличие определенных типов информационных угроз порождает соответствующие неопределенности в управлении ОС, приводящие к негативным последствиям с точки зрения достижения целей управления.

Степень неприемлемости последствий принятых решений, как правило, измеряют в условных единицах – *потерях* или *ущербе*, которые по предположению может понести субъект управления (в рассматриваемом случае – центр или агент). Основной исходной информацией, необходимой для решения задачи управления ОС в условиях неопределенности, является *функция потерь* (*ущерба*), зависящая, как и критерий эффективности, от трех аргументов: *управления* центра, *действия* агента и *обстановки* (состояния внешней и/или внутренней среды). Ключевым шагом в решении задачи является преобразование функции потерь в *функцию риска*, отражающую зависимость степени риска, уже только от одного аргумента – принимаемого управленческого решения. Способ такого преобразования неоднозначен и зависит от выбранного критерия риска. От этого же критерия зависит и смысл выражения «*наилучшее решение*»: **наилучшим называется решение, которое *минимизирует* риск**.

Применимость различных критериев риска зависит от характера неопределенности ситуации. Наиболее подробно изучены два типа таких неопределенностей: неопределенность состояний природы, то есть внешней, по отношению к организационной системе среды, и неопределенность целенаправленного противодействия субъектов, сторонних по отношению к субъекту управления, которые изучаются соответственно теорией статистических решений и теорией игр. Говоря о неопределенности состояния природы, в свою очередь, необходимо различать два случая:

- когда о фактическом состоянии природы неизвестно ничего, кроме множества, из которого оно может быть выбрано;
- когда известно распределение вероятностей (или функция плотности распределения) на множестве возможных состояний природы.

Может показаться, что «наилучшее решение» (минимизирующее выбранный критерий риска) слабо связано с «эффективным управлением» (максимизирующим выбранный критерий эффективности), однако это не так.

Действительно, рассмотрим задачу управления ОС в условиях неопределенности с выбранным критерием эффективности, зависящим от трех аргументов: *управления* центра, *действия* агента и *обстановки* (состояния внешней среды). Далее, предположим, что существует такой набор указанных аргументов («идеальная точка») при котором значение критерия эффективности становится максимальным из всех возможных. В соответствии с гипотезой рационального поведения, будем рассматривать значение критерия эффективности в «идеальной точке» в качестве *цели управления* ОС. Выберем в качестве функции ущерба разность между значениями критерия эффективности в «идеальной точке» и в точке с некоторыми текущими значениями управления, действия и обстановки (иными словами, между целью управления и реальными результатами управления)[7]. Тогда, как несложно показать (см., например, [3]), задачи **максимизации** критерия эффективности и **минимизации** функции ущерба становятся эквивалентными. Эквивалентность проявляется, прежде всего, в том, что в случае с детерминированной ОС решения обеих задач совпадают. В случае же решения задачи управления ОС в условиях неопределенности мы можем быть уверены, что выбор управляющих воздействий, **уменьшающих** значение функции риска, приводит, как правило, к **увеличению** значения критерия эффективности.

7 Необходимо отметить, что вместо значения критерия эффективности в «идеальной точке» может быть выбрано любое произвольное число, большее, чем указанное значение критерия эффективности.

4. Пути решения задачи

Все методы управления информационными рисками с точки зрения *роли информационной безопасности в организации*[8] могут быть условно разделены на две большие группы [3]: методы *организационного* управления, где в качестве объекта управления выступает субъект в организации (например, *субъект информационного процесса*[9]), и методы *технологического* управления, где в качестве объекта управления выступает объект в организации (например, *объект защиты информации*[10]).

К методам первого типа относят, как правило, *административно-процедурные, нормативно-правовые, морально-этические* и *экономические*, а к методам второго типа – *физические, технические, программные, программно-технические* и другие подобные меры и механизмы.

Все указанные меры, относящиеся к *организационному управлению*, как показано в [3], могут быть реализованы в виде определенных механизмов, относящихся к одному из трех типов управления [2]: *мотивационному*, *институциональному* или *информационному*, которые были подробно рассмотрены в работах [3, 5, 6, 7].

Среди механизмов управления, относящимися к мотивационному типу, в рамках исследования моделей управления информационными рисками в ОС были рассмотрены:

- механизмы планирования (распределения ресурса);
- механизмы стимулирования (мотивирования);
- механизмы страхования.

Среди механизмов управления, относящихся к институциональному типу, были рассмотрены:

- механизмы управления нормами деятельности;
- механизмы управления ограничениями деятельности.

Среди механизмов управления, относящихся к информационному типу, были рассмотрены:

- механизмы информационного управления;
- механизмы информационного противоборства.

Напомним, вкратце, полученные в этих работах основные результаты.

В работе [5] была рассмотрена базовая модель ОС, состоящая из пассивной внешней среды (природы), пассивного управляемого объекта и активного агента [2]. При этом было сделано дополнительное предположение о том, что множество состояний управляемого объекта можно разбить на два непустых непересекающихся подмножества: множество состояний, на которые агент может оказать управляющее воздействие, и множество состояний, на которые агент не может оказать управляющее воздействие.

В рамках анализа базовой модели была построена модель информационных угроз, в которой, учитывая предположение о «пассивности» внешней среды и управляемого объекта, были выделены три типа неопределенностей и соответствующих им типов информационных угроз:

- внешняя объективная неопределенность и соответствующее ей множество природных угроз;
- внутренняя объективная неопределенность и соответствующее ей множество техногенных угроз;
- внутренняя субъективная неопределенность и соответствующее ей множество внутренних искусственных угроз.

В качестве механизмов для их возможной нейтрализации, в рамках имеющихся у агента возможностей, были предложены [5]: для парирования природных и техногенных угроз – механизмы страхования рисков и для парирования внутренних искусственных угроз – механизмы распределения ресурса.

В соответствии с классификацией контрмер, приведенной в [3], механизмы страхования рисков могут быть отнесены к экономическим, а механизмы распределения ресурса (в случае их использования для создания технологической системы управления информационными рисками) к группе технологических контрмер.

В работе [6] была рассмотрена модель автономной ОС состоящей из активных центра и агента и пассивных внешней среды и управляемого объекта.

Поскольку, по предположению, внешняя среда

---

8 *Роль информационной безопасности в организации* – совокупность определенных функций и задач обеспечения информационной безопасности организации, устанавливающих допустимое взаимодействие между субъектом и объектом в организации. Примечания: 1) к субъектам относятся лица из числа руководителей организации, ее персонал или инициируемые от их имени процессы по выполнению действий над объектами; 2) объектами могут быть техническое, программное, программно-техническое средство, информационный ресурс, над которыми выполняются действия (см. [1], ст. 3.4.4).

9 *Информационный процесс* – процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации (см. [1], ст. 3.1.8).

10 *Объект защиты информации* – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации (см. [4], ст. 2.5.1).

является пассивной, а агент не является для центра источником угроз, модель угроз для системы «центр – агент – управляемый объект» ничем не будет отличаться от рассмотренной ранее модели угроз в системе «агент – управляемый объект». Иными словами, новых угроз не появляется. В этой связи представляет интерес вопрос о том, какие новые возможности (механизмы) управления информационными рисками появляются у центра. В соответствии с принятой моделью управления ОС центр непосредственного воздействия на управляемый объект не оказывает. Таким образом, единственным объектом управления для центра является агент. Было выделено и рассмотрено три типа возможных управляющих воздействий: *институциональное управление* (изменение *допустимых множеств* управляющих воздействий), *мотивационное управление* (изменение *функции полезности* от принятого решения) и *информационное управление* (изменение *информации*, которую агент использует при принятии решений).

В рамках мотивационного управления были рассмотрены механизмы противодействия природным и техногенным угрозам, а так же внутренним искусственным угрозам. Для противодействия природным и техногенным угрозам у центра, как и у агента в базовой модели, имеется единственная возможность – компенсация остаточных информационных рисков путем использования механизмов страхования. При этом центр может оказывать управляющие воздействия на агента либо путем задания определенных параметров для используемых механизмов страхования, либо самостоятельно использовать механизмы страхования информационных рисков, при этом механизмы, возможные для использования будут аналогичными как для центра, так и для агента.

Для противодействия внутренним искусственным угрозам, учитывая, что в данном случае центр лишен возможности самостоятельной реализации контрмер, его основной задачей становится обеспечение агента определенным объемом ресурса. Также был рассмотрен еще один вариант действий центра, направленных непосредственно на управление агентом с использованием механизмов стимулирования. С точки зрения классификации контрмер, приведенных в [3], все указанные выше действия центра относятся к классу экономических контрмер.

В рамках институционального управления были рассмотрены механизмы управления ограничениями («неписаными» правилами) деятельности агента, которые в соответствии с [3] относятся к морально-этическим контрмерам, а так же механизмы управления нормами («писаными» правилами) деятельности, которые относятся к правовым контрмерам.

Возможность информационного управления агентом в целях обеспечения управления информационными рисками в рамках данной модели у центра отсутствует.

В работе [7] была рассмотрена более сложная ситуация, когда имеются две взаимодействующие ОС, каждая из которых была построена на основе базовой модели «агент – управляемый объект» или модели «центр – агент – управляемый объект». Дополнительно было сделано предположение, что центр и агенты своими действиями могут оказывать влияние на состояние внешней среды. В этом случае в рассмотренных моделях появляется новый вид неопределенности – внешняя субъективная неопределенность и соответствующий тип угроз – внешние искусственные угрозы. Эти угрозы могут быть преднамеренными или случайными, а в качестве объектов реализации угроз может выступать либо управляемый объект, либо информация о состоянии внешней среды, иными словами – *информированность* агента.

В рамках анализа модели двух взаимодействующих организационных систем «агент – управляемый объект» была рассмотрена модель дополнительно возникающих, по сравнению с базовой моделью, информационных угроз. К этим угрозам были отнесены внешние искусственные угрозы (преднамеренные и случайные) различающиеся местом приложения: управляемый объект или информированность агента. В первом случае, представляется целесообразным рассматривать эти угрозы совместно с внутренними искусственными угрозами и использовать для их нейтрализации механизмы распределения ресурсов. Во втором случае, в соответствии с рассматриваемой моделью, единственными механизмами нейтрализации угроз являются механизмы *информационного управления*, которые предусматривают не пассивное, а активное противодействие. В этом смысле механизмы информационного управления являются скорее мерами контрнаступления и представляют собой механизмы *информационного противоборства*.

В модели двух взаимодействующих организационных систем «центр – агент – управляемый объект» появляются два новых источника угроз – центры и два новых объекта реализации угроз – информированность центров. Типы угроз (внешние искусственные угрозы) и механизмы противодействия этим угрозам (в том числе, механизмы информационного противоборства) при этом не

изменяются, но возникает проблема координации центра и агентов при реализации их совместных действий.

В модели двух взаимодействующих ОС: «центр – несколько агентов» в зависимости от того, могут ли агенты, входящие в состав одной ОС быть источниками внешних угроз друг для друга, имеем два случая:

• либо данная модель практически не будет отличаться от рассмотренной ранее модели двух взаимодействующих одноэлементных систем: «центр – агент» (в случае отсутствия взаимных угроз);

• либо потребуется дополнительное включение в рассмотрение модели двух взаимодействующих систем: «агент – управляемый объект» (при наличии взаимных угроз).

В этом случае роль центра сводится к выполнению функций своеобразного «пожарного», призванного «тушить» информационные конфликты внутри ОС путем соответствующих управляющих воздействий на участвующих в конфликтах агентов.

Анализ методов управления информационными рисками для различных моделей организационных систем, представленных в [5, 6, 7], позволил выявить определенные взаимосвязи [3]:

• между контрмерами и механизмами управления ОС, используемыми для их реализации;

• между основными классами информационных угроз и механизмами, используемыми для противодействия им.

Анализ результатов исследования механизмов управления информационными рисками ОС позволяет сделать следующие выводы [3]:

- во-первых, предлагаемый для управления информационными рисками набор, состоящий из механизмов мотивационного, институционального и информационного управления, является **полным** в том смысле, что целиком покрывает как множество классов потенциально возможных информационных угроз, так и множество всех типов контрмер. При этом конкретный вид механизма может существенно зависеть от того, кто его применяет (центр или агент) и в рамках какой модели;

- во-вторых, механизмы мотивационного управления: планирования (распределения ресурса), стимулирования и страхования в той или иной степени могут быть использованы как для реализации всех типов контрмер, так и для противодействия всем основным типам информационных угроз.

С этой точки зрения можно считать, что набор механизмов для управления информационными рисками ОС, включающий механизмы планирования, стимулирования и страхования, является **необходимым и минимально достаточным**.

Необходимость определяется тем, что исключение любого из механизмов, относящихся к мотивационному управлению, приводит к невозможности отражения всех основных типов угроз.

Минимальная достаточность определяется тем, что набор механизмов, относящихся к мотивационному управлению, позволяет в той или иной степени реализовать все основные типы контрмер, без использования механизмов управления иных типов.

Иными словами: механизмы планирования (распределения ресурса), стимулирования и страхования представляют собой группу **основных** (или **базовых**) механизмов управления информационными рисками ОС, а механизмы управления ограничениями и нормами деятельности, а также механизмы информационного управления (в том числе – информационного противоборства) представляют собой группу **вспомогательных** механизмов управления информационными рисками ОС.

5. Заключение

Указанный выше набор моделей и механизмов с дополнительным включением механизмов контроля, позволяет реализовать законченный цикл организационного управления информационными рисками

Механизмы планирования, стимулирования и страхования могут оказывать влияние на величину информационных рисков, в частности, способствовать ее снижению.

Механизмы контроля не оказывают влияние на величину информационных рисков, но позволяют установить уровень допустимого риска и осуществлять мониторинг отклонений от этого значения.

Необходимо отметить, что в настоящее время намечены только общие контуры подхода к проблеме управления информационными рисками объектов КИИ РФ. В частности, мало исследованным остается вопрос использования механизмов информационного управления, в том числе – информационного противоборства. Данное обстоятельство открывает широкую перспективу для дальнейших исследований в данном направлении.

Литература

1. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2009. – 20 с.
2. Новиков Д.А. Теория управления организационными системами. 3-е изд. – М.: Издательство физико-математической литературы, 2012. – 604 с.
3. Калашников А.О. Модели и методы организационного управления информационными рисками корпораций. М.: Эгвес, 2011. – 312 с.
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2010. – 8 с.
5. Калашников А.О. Управление информационными рисками организационных систем: базовая модель // Системы управления и информационные технологии. – 2008. – № 1.3(31). – С. 366 – 371.
6. Калашников А.О. Управление информационными рисками автономных организационных систем // Системы управления и информационные технологии. – 2008. – № 2.2 (32). – С. 262 – 267.
7. Калашников А.О. Управление информационными рисками взаимодействующих организационных систем // Системы управления и информационные технологии. – 2008. – № 1.3(31). – С. 375 – 380.

References

1. GOST R 53114-2008. Zashchita informatsii. Obespechenie informacionnoy bezopasnosti v organizacii. Osnovnie termini I opredeleniya. – M.: Standartinform, 2009. – 20 s.
2. Novikov D.A. Teoriya upravleniya organizacionnimi sistemami. 3-e izd. – M.: Izdatelstvo fiziko-matematicheskoy literaturi, 2012. – 604 s.
3. Kalashnikov A.O. Modeli i metodi organizacionnogo upravleniya informatsionnimi riskami korporatsii. – M.: Egves, 2011. – 312 s.
4. GOST R 50922-2006. Zashchita informatsii. Osnovnie termini I opredeleniya. – M.: Standartinform, 2009. – 8 s.
5. Kalashnikov A.O. Upravlenie informatsionnimi riskami organizacionnih system: bazovaya model // Sistemi upravleniya i informacionnie tehnologii. – 2008. – № 1.3(31). – P. 366 – 371.
6. Kalashnikov A.O. Upravlenie informatsionnimi riskami avtonomnih organizacionnih system // Sistemi upravleniya i informacionnie tehnologii. – 2008. – № 2.2 (32). – P. 262 – 267.
7. Kalashnikov A.O. Upravlenie informatsionnimi riskami vzaimodeystvuyuschih organizacionnih system // Sistemi upravleniya i informacionnie tehnologii. – 2008. – № 1.3(31). – P. 375 – 380.