DOI 10.37882/2223-2966.2023.07.29

МОДЕЛИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ «ВЫБОР СРЕДСТВ ЗАЩИТЫ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР» НА ОСНОВАНИИ ВЛИЯНИЯ ВНЕШНЕЙ СРЕДЫ

SIMULATION OF THE CONTROL SYSTEM «CHOICE OF PROTECTION MEANS FOR OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURES» BASED ON EXTERNAL INFLUENCE

K. Pestrakova

Summary: A methodology for modeling the control system «Choice of protection means for CII objects» has been developed. The model of the control system is presented and its description is given. The problem of optimal control of the developed system is formulated.

Keywords: control system, control system model, control object, control subject, external environment, critical information infrastructures, objects of critical information infrastructures.

Пестракова Кристина Александровна
Аспирант, Брянский государственный технический университет
kris.siniczckaia@yandex.ru

Аннотация: Разработана методика моделирования системы управления «Выбор средств защиты для объектов КИИ». Представлена модель системы управления и дано ее описание. Сформулирована задача оптимального управления разработанной системы.

Ключевые слова: система управления, модель системы управления, объект управления, субъект управления, внешняя среда, критические информационные инфраструктуры, объекты критических информационных инфраструктур.

С каждым годом все актуальнее становятся проблемы, связанные с безопасностью информационных систем, данная ситуация объясняется ростом показателей инцидентов информационной безопасности, высокими показателями внедрения в различные сферы информационных технологий, и, конечно же увеличением случаев угроз, направленных на безопасность информации. Внедрение информационных технологий и обеспечение их безопасности наиболее востребованы в таких сферах, как банковская сфера, сфера здравоохранения, связи, транспорта, энергетики, сфера атомной энергии, оборонной, химической промышленности и других сферах. Данные сферы являются важными государственными областями и в таком случае потребность в обеспечении защиты информационных систем от угроз и атак это необходимое условие к предоставлению новых требований к объектам критических информационных инфраструктур (далее КИИ) [1,5].

Обеспечение безопасности на протяжении всего жизненного цикла объектов КИИ является важной и неотъемлемой задачей защиты информации. На субъекты КИИ возлагается право на определение требований безопасности объектов КИИ и на выбор мер и средств по их защите. При определении данных требований также должны учитываться категории значимости объектов КИИ [6,8]. Для решения обозначенных вопросов необходимо разработать новые методы, модели и методики, которые помогут специалистам, ответственным за обеспечение безопасности значимых объектов КИИ в кратчайшие сроки провести процедуру категорирования, оценки защищенности и выбора средств защиты для объектов КИИ. При этом для повышения эффективности и оптимизации процесса выбора средств защиты для объектов КИИ в соответствии с их категорией значимости целесообразно процедуру выбора автоматизировать, интегрировав в формальную систему, позволяющую на основе разработанных подходов выполнить требования по защите в соответствии с законодательством.

В рамках данной работы и на начальном этапе исследования разработана методика моделирования системы управления Выбор средств защиты для объектов КИИ (далее СУ ВСЗоКИИ), которая включается в себя описание модели системы управления, формулировку задачи оптимального управления данной системы. В дальнейшей работе планируется выявить критериев оптимальности и определить соответствующие ограничения.

Для всестороннего исследования проблем управления выбором средств защиты для объектов КИИ и при этом учитывая требования ФСТЭК, ФСБ и отраслевых регуляторов актуально применение инструментов теории управления. В данной трактовке формулируются условия для эффективного выбора средств защиты для объектов КИИ, учитывающих требования ФСТЭК, ФСБ и отраслевых регуляторов, а также предполагаемые управляющие воздействия по выполнению желаемых

результатов [7]. Управление выбором средств защиты для объектов КИИ на базе принципов и понятий теории управления учитывает динамику и обеспечивает объективную оценку возникающих изменений в объекте управления под воздействием внешней среды, возмущения которой изменяют задающее воздействие требования ФСТЭК, ФСБ и отраслевых регуляторов, что может привести к расхождению с поставленными целями [4]. Поэтому возникает необходимость в предоставлении программы для быстрого принятия корректирующих управленческих решений, с учетом влияния внешней среды и наблюдение несоответствия с требованиями ФСТЭК, ФСБ и отраслевых регуляторов [2].

Необходимо учитывать особенности функционирования системы управления при выборе средств защиты для объектов КИИ, поэтому в данном исследования предложена индивидуальная разработка методологии управления социально-экономическими системами. Для этого в предложенной методологии по отношению к разработанной СУ ВСЗоКИИ введены понятия и термины, которые также используют в теории управления. Важно отметить, что в предложенной методологии расписана не только структура этапов, но и представлены содержание и методика выбора средств защиты объектов КИИ на основе анализа внешней среды.

Разработанная методология управления выбором средств защиты объектов КИИ на основании анализа воздействия внешней среды и, учитывая критерии значимости объектов КИИ:

Этап 1: Формализация задающего воздействия требований ФСТЭК, ФСБ и отраслевых регуляторов в СУ ВСЗоКИИ.

Методика 1: Формализация задающего воздействия требований ФСТЭК, ФСБ и отраслевых регуляторов в СУ ВСЗоКИИ.

Содержание методики 1:
1. Определение основных задач и требований ФСТЭК, ФСБ и отраслевых регуляторов в качестве задающего воздействия СУ ВСЗоКИИ.
2. Сопоставление требований ФСТЭК, ФСБ и отраслевых регуляторов с основными этапами выбора средств защиты для объектов КИИ для дальнейшего определения управленческого воздействия.
3. Выявление требований ФСТЭК, ФСБ и отраслевых регуляторов, которые учитываются при классификации выбора средств защиты для объектов КИИ.
4. Определение главных требований ФСТЭК, ФСБ и отраслевых регуляторов (на которые стоит обратить внимание в первую очередь) и их предназначение в модели СУ ВСЗоКИИ.

Этап 2: Проецирование главных связей и компонентов СУ ВСЗоКИИ.

Методика 2.1: Моделирование СУ ВСЗоКИИ.

Содержание методики 2.1:
1. Построение модели СУ ВСЗоКИИ.
2. Разработка задачи оптимального управления в СУ ВСЗоКИИ.
3. Выбор критериев оптимальности.
4. Введение ограничений.

Методика 2.2: Характеристика объекта управления.

Содержание методики 2.2:
1. Порядок создания модели объекта управления СУ ВСЗоКИИ.
2. Классификация модели объекта управления с учетом предложенного подхода.
3. Создание модели выходных параметров объекта управления.

Методика 2.3: Обзор внешней среды.

Содержание методики 2.3:
1. Устройство модели внешней среды для выбора средств защиты объектов КИИ.
2. Классификация факторов внешней среды.
3. Создание модели возмущений внешней среды.
4. Анализ воздействия внешней среды на выбор средств защиты для объектов КИИ.

Этап 3: Исследование внешней среды.

Методика 3: Оценка состояния внешней среды в данный момент времени.

Содержание методики 3:
1. Создание модели измерительных устройств.
2. Анализ влияния измерительных устройств на составляющие СУ ВСЗоКИИ.
3. Определение количества связей, влияющих на СУ ВСЗоКИИ.
4. Генерирование ситуаций, на которые следует обратить внимание.
5. Построение модели возмущений на управляющее устройство, которые поступают от измерительных устройств.

Этап 4: Функция контроля в СУ ВСЗоКИИ.

Методика 4: Контроль состояния объекта управления в определенный промежуток времени и в конечном состоянии.

Содержание методики 4:
1. Создание модели функции контроля в СУ ВСЗоКИИ.

2. Проведение контроля в определенный промежуток времени в СУ ВСЗоКИИ.
3. Проведение контроля в конечном состоянии в СУ ВСЗоКИИ.

Этап 5: Назначение управленческих решений по выбору средств защиты для объектов КИИ с привлечение ресурсов СППР «Выбор» и учитывая задающее воздействие ФСТЭК, ФСБ и отраслевых регуляторов.

Методика 5: Обеспечение принятия управленческих решений по выбору средств защиты для объектов КИИ с учетом задающего воздействия на основании проведенного анализа влияния внешней среды.

Содержание методики 5:

1. Исследование управленческой ситуации, учитывая требования ФСТЭК, ФСБ и отраслевых регуляторов и влияние внешней среды.
2. Анализ управленческих проблем выбора средств защиты для объектов КИИ, при воздействии ФСТЭК, ФСБ и отраслевых регуляторов и внешней среды.
3. Определение альтернативного набора управленческих решений.
4. Подбор критериев для выбора решений из уже имеющихся альтернатив.
5. Учитывая набор сформированных критериев определение лучшего управленческого решения.
6. Реализация управленческого решения в отношении выбора средств защиты для объектов КИИ (конкретные действия).

В результате, разработанная методологии управления выбора средств защиты для объектов КИИ с учётом их категории значимости и на основании исследования внешней среды, даёт возможность реализовать процесс принятия управленческих решений выбора средств защиты для объектов КИИ с использованием разработанной СППР «Выбор» под воздействием требований ФСТЭК, ФСБ и отраслевых регуляторов и контролем НКЦКИ.

Модель системы управления ВСЗоКИИ представлена на рис. 1.

Модель СУ Выбор средств защиты для объектов КИИ в общем виде может быть представлена следующим множеством с использованием теоретико-множественного подхода (1):

$$СУ_{ВСЗоКИИ} = \{M, X, Y, Z, D\} \quad (1)$$

где M — множество компонентов $СУ_{ВСЗоКИИ}$ (2),

$$M = \left\{CO, CD, ED, EE, KD, \left\{MD_{\omega} \mid \omega = 1.2\right\}\right\} \quad (2),$$

где *CO* — объект управления (*control object*), *CD* — управляющее устройство (система поддержки принятия решений «Выбор» (*control device*)), *ED* — исполнительное устройство (абстрактный специалист по ИБ (*executive device*)), *EE* — внешняя среда (*external environment*), *KD* — контролирующее устройство (control device), MD_{ω} — два измерительных устройства (*measuring devices*), *X* — матрица управляющего воздействия, *Y* — матрица выход-

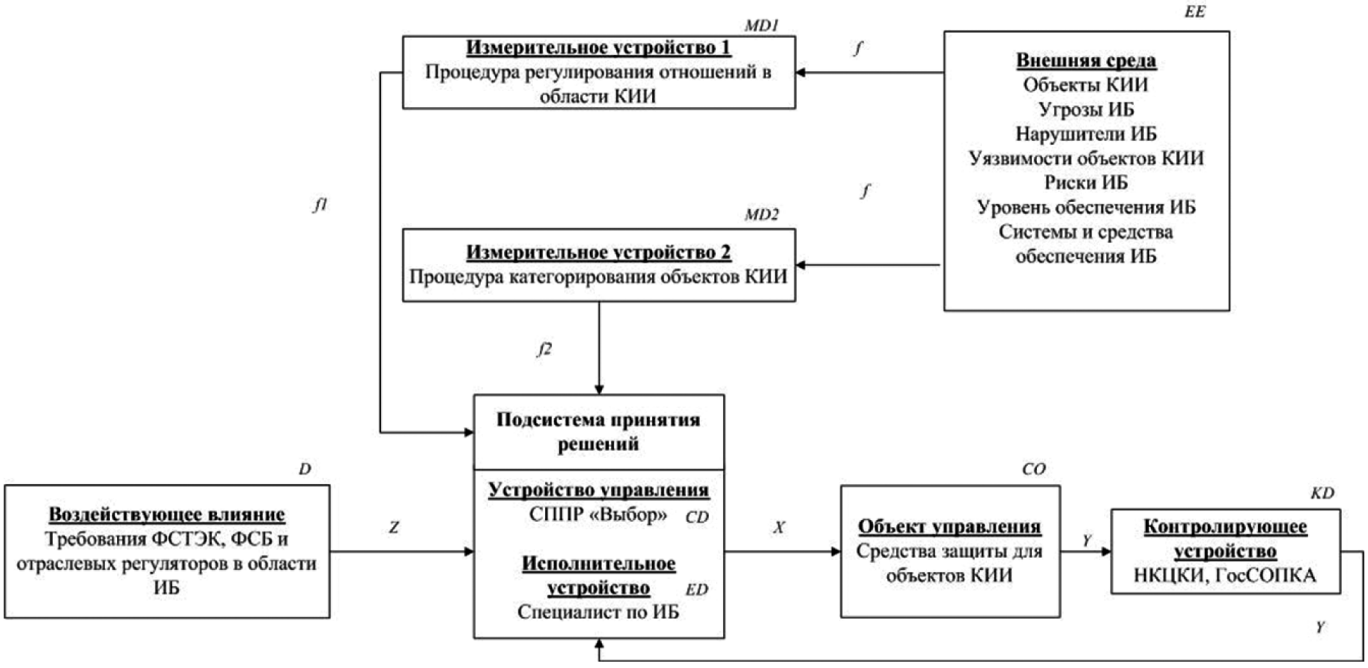

Рис. 1. Модель системы управления выбора средств защиты для объектов критических информационных инфраструктур

ных координат, *Z* — матрица задающего воздействия, *D* — множество воздействий внешний среды на объект управления через управляющее устройство.

Задающее воздействие *Z* в разработанной СУ ВСЗоКИИ представлено требованиями ФСТЭК, ФСБ и отраслевых регуляторов. Формализация задающего воздействия *Z* требований ФСТЭК, ФСБ и отраслевых регуляторов в СУ ВСЗоКИИ прописана в разработанной методологии. Задающее воздействие *Z* в первую очередь поступает на подсистему принятия решений, далее оно функционирует в операциях управляющего воздействия *X* и оказывает влияние на объект управления.

Управляющее воздействие *X* показывает ряд операций действующих в рамках требований ФСТЭК, ФСБ и отраслевых регуляторов. Особенности контролирующих устройств определяют выходные координаты. Что касаемо внешней среды *EE*, она создает возмущающие внешние воздействия, учитываемые подсистемой принятия решений. Информация, которая поступает из внешней среды на объект управления, переходит к измерительным устройствам (MD_1, MD_2). Измерительные устройства обрабатывают полученные данные и информируют о важности анализируемого влияния внешней среды на объект управления. Принятие во внимание факторов внешней среды происходит при помощи ряда правил, представляющие собой логические правила выбора корректирующих мероприятий (управленческих решений), повышения эффективности, оптимизации процесса выбора средств защиты.

Подсистема принятия решений состоит из управляющего устройства, которое представлено СППР «Выбор» и исполнительного устройство, которое представлено абстрактным специалистом по информационной безопасности. С помощью измерительного устройства СППР «Выбор» производит обработку информации о внешней среде в данный момент времени. Специалист по ИБ является пользователем СППР «Выбор». При проведении процедуры принятия управленческих решений для формирования матрицы управляющего воздействия специалист по ИБ обращается к СППР «Выбор». Программное обеспечение построено таким образом, что специалист по ИБ может быть недостаточно компетентен в вопросах моделирования и программирования, но при этом он быстро и четко сможет проанализировать, как внешняя среда влияет на объект управления, вычислить временной фактор принятия решений и выполнить корректирующие управленческие решения для реализации требований ФСТЭК, ФСБ и отраслевых регуляторов [4].

Задачу оптимального управления в СУ ВСЗоКИИ можно определить следующим образом. Под влиянием задающего воздействия требований ФСТЭК, ФСБ, отраслевых регуляторов в области ИБ необходимо подобрать такую последовательность действий, при которой объект управления (Средства защиты для объектов КИИ) получая информацию из внешней среды и учитывая возмущающие воздействия (Процедура регулирования отношений в области КИИ, процедура категорирования объектов КИИ) переходит из состояния начального момента (незащищенные объекты КИИ) в конечное состояние (защищенные объекты КИИ), при этом выполняется ряд правил, представляющих собой логические правила выбора корректирующих мероприятий (управленческих решений), повышения эффективности, оптимизации процесса выбора средств защиты[3].

ЛИТЕРАТУРА

1. Аверченкова, Е.Э. Модель информационной безопасности информационной советующей системы / Е.Э. Аверченкова, Д.И. Гончаров, Д.А. Лысов // Вестник Брянского государственного технического университета. — 2016. — №4(52). — С. 251–261.
2. Аверченкова, Е.Э. Методология управления региональной социально-экономической системой на основе анализа влияния внешней среды [Текст]: автореф. дис. … д-ра. техн. наук: 05.13.10/ Аверченкова Елена Эдуардовна. — Волгоградский государственный технический университет, 2020. — 380 с.
3. Балдин, К.В. Управленческие решения: Теория и технологии принятия: учебник для вузов/ К.В. Балдин, С.Н. Воробьев. — М.: Проект, 2004 г.
4. Васильев Д.К., Заложнев А.Ю., Новиков Д.А., Цветков А.В. Типовые решения в управлении проектами. — М.: ИПУ РАН, 2003.
5. Горелик, В.Ю. О безопасности критической информационной инфраструктуры Российской Федерации/ В.Ю. Горелик, М.Ю. Безус// Научно-образовательный журнал для студентов и преподавателей «StudNet». — 2020. — №9. — С. 1438–1448.
6. Постановление Правительства Российской Федерации №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»: [утверждено постановлением Правительства Российской Федерации 8 февраля 2018 г.] — СПб.: Стаун-кантри, 2018 — 17 с.
7. Приказ ФСТЭК России №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»: [утверждено приказом ФСТЭК России 25 декабря 2017 г.] — СПб.: Стаун-кантри, 2017 — 34 с.
8. Федеральный закон Российской Федерации №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: [федер. закон: принят Гос. Думой 12 июля 2017 г.] — СПб.: Стаун-кантри, 2017 — 15 с.

Журнал «Современная наука: актуальные проблемы теории и практики»