

Прокопенко А.Н., канд. техн. наук, проф.
Белгородский юридический институт МВД России им. И.Д. Путилина
Ковалева Е.Г., канд. техн. наук,
Васюткина Д.И., ассистент

Белгородский государственный технологический университет им. В.Г. Шухова

СИСТЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ИНФОРМАЦИОННЫХ СИСТЕМ

zchs@intbel.ru

Проведен анализ системы организационно-технического управления комплексной безопасностью высшего учебного заведения и разработана функциональная модель процесса организационно-технического управления комплексной безопасностью с применением IDEF технологий.

Ключевые слова: безопасность, комплексная безопасность, иерархия, информационная система, риск, модель.

Введение. Система организационно-технического управления (СОТУ) высшего учебного заведения предназначена для оценки для оценки текущего состояния и определения целевого уровня безопасности, планирования мероприятий в рамках финансирования, анализа риска, определение архитектуры комплекса технических средств безопасности, определение направлений модернизации СОТУ и мониторинга функционирования системы управления при защите учреждений от внешних угроз различного характера – террористической, пожарной, экологической и других [1].

Оперативное управление системами жизнеобеспечения и системами безопасности (СБ) в штатных ситуациях может осуществляться с помощью управляющих программ, разработанных на основе известных алгоритмов [2]. Однако, если в результате аварии или реализации внешних угроз возникает чрезвычайная ситуация (ЧС), такое управление становится неэффективным из-за неполноты и неопределенности исходной информации, а также плохой структурируемости возникающей обстановки.

Обычное управление не позволяет своевременно принять решения по локализации опасных событий и смягчению их поражающих воздействий, по организации взаимодействия оперативных служб учреждения и города, направленного на устранение ЧС и ликвидацию ее последствий.

Сложность осуществления эффективного управления в трудно формализуемых ЧС привела к необходимости разработки процесса организационно-технического управления безопасностью высшего учебного заведения на основе IDEF технологий [3].

Методология. В процессе работы был использован системный подход, охватывающий методы обобщения и анализа, аналитические исследования, методы математического моделирования.

Основная часть. Система организационно-технического управления (СОТУ) безопасностью ВУЗа – это часть общей системы управления ВУЗом, направленная на создание, обеспечение, управление, мониторинг, контроль, поддержание и улучшение комплексной безопасности ВУЗа. Как следует из определения, в качестве объекта управления СОТУ выступает система обеспечения комплексной безопасности ВУЗа. А, как было отмечено в 1-й главе, система управления безопасностью ВУЗа является необходимым элементом системы менеджмента качества ВУЗа [4].

Система управления качеством функционирования ВУЗа вырабатывает управляющие воздействия С для различных составляющих деятельности ВУЗа. Результатом данных воздействий является достижение ВУЗом определенного качества функционирования К. Данное значение достигается, в том числе, за счет обеспечения системой ОТУ безопасностью ВУЗа заданного значения уровня обеспечения безопасности УБ. В качестве входных параметров Х для СОТУ выступает информация о категории ВУЗа, ресурсах ВУЗа, финансовых ограничениях. СОТУ, в свою очередь, формирует определенный состав СОКБ, направляя командную информацию U для всех составляющих СОКБ. Эффективность функционирования данных составляющих E, в первую очередь КТСБ, служит основой для СОТУ при определении текущего уровня обеспечения безопасности ВУЗа.

Для того чтобы определить архитектуру СОТУ, необходимо выявить круг решаемых ею задач. С этой целью воспользуемся подходом, описанным в стандарте ИСО 27001, в соответствии с которым процесс создания, обеспечения, управления, мониторинга, контроля, поддержания и улучшения комплексной безопасности ВУЗа должен осуществляться в рамках 4-хфазной модели PDCA (Plan-Do-Check-Act). Модель PDCA (или модель Шухарта-Деминга) определяет четыре

этапа, которые должны выполняться последовательно на каждом этапе жизненного цикла СОТУ [5]:

1. Планируй (создание СОТУ).
2. Выполняй (внедрение и функционирование СОТУ).
3. Проверяй (мониторинг и проверка СОТУ).
4. Действуй (поддержание и улучшение СОТУ).

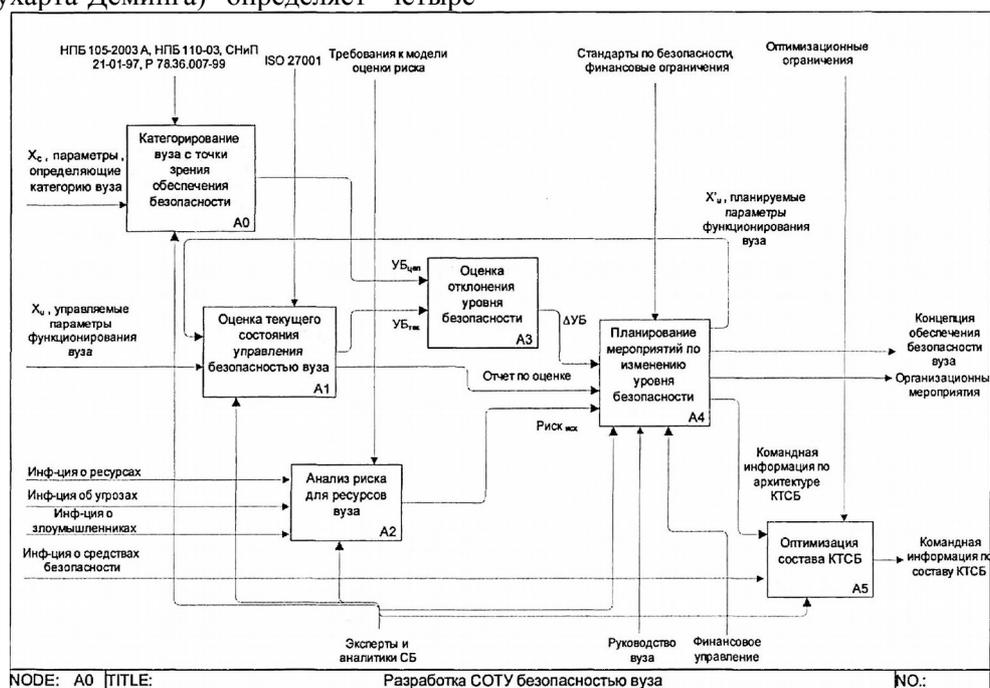


Рис. 1. Функциональная модель процесса организационно-технического управления безопасностью ВУЗа

Жизненный цикл СОТУ:

1. Начальным шагом при создании СОТУ является выпуск приказа о намерении создать систему организационно-технического управления безопасностью ВУЗа с указанием ответственных лиц, ориентировочных сроков выполнения подготовительных мероприятий.

В соответствии с приказом создается команда проекта или же целое подразделение, ответственное за непрерывное обеспечение безопасности ресурсов ВУЗа. Дальнейшие этапы проекта лежат в рамках подхода РОСА.

2. Планируй: разработка Концепции обеспечения безопасности, включающей:

2.1 Категорирование ВУЗа с точки зрения обеспечения безопасности;

2.2 Качественную оценку текущего состояния обеспечения безопасности и определение целевого уровня обеспечения безопасности;

2.3 Выявление направлений создания (совершенствования) СОТУ;

2.4 Планирование мероприятий в рамках выявленных направлений в соответствии с возможностями финансирования;

2.5 Количественную оценку риска (идентификация ресурсов, подлежащих защите, угроз и моделей злоумышленника, уязвимостей, расчет потенциальных потерь);

2.6 Политику управления рисками:

- принятие рисков — значения приемлемых рисков;

- избегание рисков — возможности по исключению влияния угроз на ресурсы;

- применение соответствующих средств снижения рисков;

2.7 Выбор средств снижения рисков в соответствии с требованиями нормативных документов и пожеланиями Заказчика (в том числе организационных мер);

2.8 Определение архитектуры комплекса технических средств безопасности по подсистемам;

2.9 Определение требований к интеграции подсистем;

2.10 Выбор оптимального состава КТСБ;

2.11 Разработка технических заданий (ТЗ) на КТСБ в целом и отдельные подсистемы.

3. Выполняй:

3.1 Производство закупок необходимых работ в соответствии с планом мероприятий и выделяемым финансированием;

3.2 Монтаж и ввод в эксплуатацию оборудования подсистем КТСБ;

3.3 Интеграция подсистем в соответствии с требованиями, приведенными в концепции.

4. Проверь:

4.1 Периодическая оценка достигнутого рейтинга (уровня) обеспечения безопасности;

4.2 Мониторинг функционирования КТСБ с помощью вспомогательной системы поддержки принятия решений [6].

5. Действуй:

5.1 Замена оборудования, вышедшего из строя;

5.2 Изменение желаемого уровня безопасности;

5.3 Модернизация СОТУ.

Функциональная модель процесса организационно-технического управления безопасностью ВУЗа, построенная с применением ЮЕИ-технологии [7], представлена на рис. 1

Выводы. Таким образом, проведенное исследование направлено на повышение эффективности организационно-технического управления комплексной безопасностью ВУЗа путем разработки соответствующего методического обеспечения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Радоуцкий В.Ю., Шаптала В.Г., Шульженко В.Н., Добровольский В.С., Овечкин

А.Н. Комплексная безопасность высших учебных заведений: монография. Петербург: Изд-во «Инфо - да», 2008. 120с.

2. Борисов В.В., Парфенов В.Н., Вохмянин В.В., Сютин Ю.С. Модель жизнеобеспечения муниципальных образований // Тезисы докладов 10-ой международной научно – практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. Москва, ЦСМ МЧС России, 19-21 апреля 2005г. С. 38 - 39.

3. Поспелов Д.А. Ситуационное управление – основа прикладных интеллектуальных систем // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». 1995. №2. С. 22– 30.

4. Радоуцкий В.Ю., Шаптала В.Г., Ветрова Ю.В. Управление комплексной безопасностью высших учебных заведений: монография. Белгород: Изд-во БГТУ, 2013. 125с.

5. Security Lifecycle - Managing the Threat, http://www.sans.org/reading_room/whitepapers/basics/security_lifecycle_managing_the_threat_592

6. Шаптала В.Г., Радоуцкий В.Ю., Шаптала В.В. [Системы информационной поддержки принятия управленческих решений при ликвидации последствий чрезвычайных ситуаций органами управления ВУЗа // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2012. № 4. С. 188–191.](#)

7. Черемных, С.В., Семенов, И.О., Ручкин, В.С. Моделирование и анализ систем. IDEF-технологии: практикум. М.: Финансы и статистика, 1997. 188 с.

Prokopenko A.N., Kovaleva E.G., Vasyutkina D.I.

OPERATIONAL CONTROL SYSTEM OF INTEGRATED SAFETY ON THE BASIS OF INFORMATION SYSTEMS

The analysis of organizational and technical control system of higher education institutions' integrated safety has been carried out and the functional model of organizational and technical control process of integrated security with the use of IDEF-technologies has been developed.

Key words: *safety, integrated safety and security, hierarchy, information system, risk, model.*

Прокопенко Алексей Николаевич, кандидат технических наук, доцент, начальник кафедры ИКТД ОВД.

Белгородский юридический институт МВД России им. И.Д. Путилина.

Адрес: Россия, 308024, Белгород, ул. Горького, 71.

E-mail: zchs@intbel.ru.

Ковалева Екатерина Геннадьевна, кандидат технических наук, старший преподаватель кафедры защиты в чрезвычайных ситуациях.

Белгородский государственный технологический университет им. В.Г. Шухова.

Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46

E-mail: kovalevazchs@yandex.ru

Васюткина Дарья Игоревна, ассистент кафедры защиты в чрезвычайных ситуациях.

Белгородский государственный технологический университет им. В.Г. Шухова.

Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46

E-mail: dasha_bgty@mail.ru