LOW-POWER REPEATER BASED ON CROSS POLARIZED RADIATORS

Maslov O.N., Khuako R.A.

The possibility of designing a low-power dual-polarization repeater based on cross-polarized radiators, description of the model and the results of its tests are considered.

Keywords: *repeater, transmitter, amplifier, antenna polarization.*

Маслов Олег Николаевич, д.т.н., профессор, заведующий Кафедрой экономических и информационных систем Поволжского государственного университета телекоммуникаций и информатики. Тел. 8-902-371-06-24. E-mail: maslov@psati.ru

Хуако Руслан Асланович, инженер 1-ой категории ОАО НИРТИ (г. Калуга). Тел. 8-903-636-10-51; 8-910-915-92-21. E-mail: bgd49@mail.ru

УДК 621.396.4

СОВРЕМЕННЫЕ МЕТОДИКИ, ПРИМЕНЯЕМЫЕ ДЛЯ ОЦЕНКИ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

Губарева О.Ю., Пугин В.В.

Современным информационным системам доверяют решение самых разнообразных и важных задач: автоматизированное управление технологическими процессами и промышленными предприятиями, автоматизацию деятельности банков, финансовых бирж, страховых и торговых компаний и так далее. Растут масштабы и сложность корпоративных систем. Важность задачи обеспечения безопасности корпоративных информационных ресурсов осознана как руководством компаний, так и их клиентами. И уже недостаточным условием является организация защиты отдельных сегментов информационной системы. Исходя из этого требования информационной безопасности должны быть направлены на обеспечение оптимального режима функционирования информационной системы в целом.

Ключевые слова: информационная безопасность, информационная система, риск, анализ, методика, контрмера, защищенность, модель, аудит, угроза, уязвимость.

Введение

Построение практически любой системы информационной безопасности (ИБ) должно начинаться с анализа рисков. Прежде чем проектировать систему ИБ, необходимо точно определить, какие угрозы (т. е. условия и факторы, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный доступ к ней) существуют для данной информационной системы (ИС) и насколько они потенциально опасны.

Грамотный учет существующих угроз и уязвимостей ИС, выполненный на этой основе анализ рисков закладывают основу для выбора решений с необходимым уровнем ИБ при минимальных затратах [1].

Аудит безопасности целесообразно проводить: при подготовке технического задания на проектирование и разработку системы защиты информации; после внедрения системы безопасности для оценки уровня ее эффективности; для систематизации и упорядочения существующих мер защиты информации; для расследования произошедшего инцидента, связанного с нарушением информационной безопасности; а также для приведения действующей системы безопасности в соответствие требованиям российского или международного законодательства [2].

Все существующие и используемые на сегодняшний день методики для оценки рисков можно условно разделить на несколько групп [4]:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP;
- количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.).

Методика ГРИФ 2005 компании Digital Security

На российском рынке распространены отечественные разработки компании Digital Security – ГРИФ и КОНДОР [9]. Рассмотрим алгоритм работы

данного продукта на примере ГРИФ 2005 из состава Digital Security Office.

Оценка риска ИБ по методики ГРИФ осуществляется с помощью построения модели ИС организации. Рассматривая средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации.

В результате работы алгоритма программа представляет следующие данные:

- инвентаризацию ресурсов;
- значения риска для каждого ценного ресурса организации;
- значения риска для ресурсов после задания контрмер (остаточный риск);
- эффективность контрмер;
- рекомендации экспертов.

Для того чтобы оценить риск информации, необходимо проанализировать защищенность и архитектуру построения ИС.

Перейдем непосредственно к работе алгоритма модели, где риск оценивается отдельно по каждой связи «группа пользователей – информация», то есть модель рассматривает взаимосвязь «субъект – объект», учитывая все их характеристики.

Риск реализации угрозы ИБ для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Владелец информации задает ущерб отдельно по трем угрозам; это проще и понятнее, так как оценить ущерб в целом не всегда возможно.

В математическом виде эта методика представляется следующим образом. Из суммы итоговой вероятности реализации угрозы получается выражение для расчета риска конкретного вида информации с учетом всех групп пользователей, имеющих к ней доступ:

$$P_{\text{inf}} = 1 - \prod_{i=1} (1 - P_{ug,n}) .$$

Затем полученная итоговая вероятность для информации умножается на ущерб от реализации угрозы, получая, таким образом, риск от реализации угрозы для данной информации. Чтобы получить риск для ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

Специфичный параметр для связки «информация – группа пользователей» – время простоя сетевого оборудования. Доступ к ресурсу может осуществляться разными группами пользователей, используя разное сетевое оборудование. Для сетевого оборудования время простоя задает владелец ИС. Время простоя сетевого оборудования суммируется со временем простоя информации, полученным в результате работы алгоритма, таким образом, мы получаем итоговое время простоя для связи «информация – группа пользователей».

Значение времени простоя для информации T_{inf}, учитывая все группы пользователей, имеющих к ней доступ, вычисляется по следующей формуле:

$$T_{\text{inf}} = (-\prod_{i=1}^{n} (1 - \frac{T_{ug,n}}{T_{\max}})) \times T_{\max}$$

где $T_{\max}$ – максимальное критичное время простоя; $T_{ug,n}$ – время простоя для связи «информация – группа пользователя».

Перемножая итоговое время простоя и ущерб от реализации угрозы, получим риск реализации угрозы «отказ в обслуживании» для связи «информация – группа пользователей».

Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. То есть на выходе пользователь получает значение двух рисков: риска без учета контрмеры R_{old} и риск с учетом заданной контрмеры R_{new}.

Эффективность E введения контрмеры рассчитывается по следующей формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}} .$$

Для оценки рисков ИС организации защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

К недостатку ГРИФ можно отнести: отсутствие возможности добавить специфичные для данной компании требования политики безопасности.

Методика Facilitated Risk Analysis Process (FRAP)

Разработана компанией Peltier and Associates [5] рассматривает обеспечение ИБ ИС в рамках процесса управления рисками. Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы. После завер-

шения оценки проводится анализ соотношения затрат и получаемого эффекта (англ. cost/benefit analysis), который позволяет определить те средства защиты, которые нужны для снижения риска до приемлемого уровня.

В FRAP раскрываются пути получения данных о системе и ее уязвимостях [9].

При проведении анализа принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом, оценивается уровень риска для незащищенной ИС, что впоследствии позволяет показать эффект от внедрения средств защиты информации (СЗИ).

Методика CRAMM

Метод CRAMM [7] основан на комплексном подходе к оценке рисков, который сочетает количественные и качественные методы анализа. Метод подходит как для крупных, так и для малых организаций как правительственного, так и коммерческого сектора, так как является универсальным методом. Программное обеспечение CRAMM ориентировано на разные типы организаций, отличием которых являются базы знаний (profiles). К примеру, правительственный вариант профиля (Government profile) позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC («Оранжевая книга»). Снимок экрана CRAMM для сводной оценки рисков недоступности двух информационных подсистем приведен на рис. 1.

Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения. Ценность данных и программного обеспечения определяется в следующих ситуациях:

- недоступность ресурса в течение определенного периода времени;
- разрушение ресурса – потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация – рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
- ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу;
- 6 баллов – от $1000 до $10 000;
- 8 баллов – от $10 000 до $100 000;
- 10 баллов – свыше $100 000.

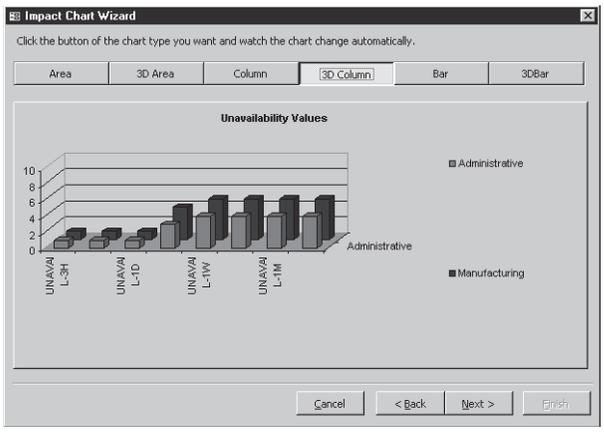

Рис. 1. Пример сводной оценки рисков недоступности двух информационных подсистем

Уровень угроз оценивается в зависимости от ответов на список вопросов, сгенерированный программным обеспечением CRAMM для каждой группы ресурсов как очень высокий, высокий, средний, низкий и очень низкий.

CRAMM – пример методики расчета, при которой первоначальные оценки даются на качественном уровне и потом производится переход к количественной оценке (в баллах).

Методика Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE – методика поведения оценки рисков в организации, разрабатываемая институтом Software Engineering Institute (SEI) при Университете Карнеги Меллон (Carnegie Mellon University) [6].

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

OCTAVE предполагает три фазы анализа:

- разработка профиля угроз, связанных с активом;
- идентификация инфраструктурных уязвимостей;
- разработка стратегии и планов безопасности.

При описании профиля в методике OCTAVE предлагается использовать «деревья вариантов», пример одного из таких деревьев изображен на рис. 2.

При создании профиля угроз рекомендуется избегать обилия технических деталей – это задача

второго этапа исследования. Главная задача первой стадии – стандартизованным образом описать сочетание угрозы и ресурса.

В OCTAVE при оценке риска дается только оценка ожидаемого ущерба, без оценки вероятности, в виде шкалы: высокий (high), средний (middle), низкий (low). Оценивается финансовый ущерб, ущерб репутации компании, жизни и здоровью клиентов и сотрудников, ущерб, который может вызвать судебное преследование в результате того или иного инцидента. Описываются значения, соответствующие каждой градации шкалы (например, для малого предприятия финансовый ущерб в $10000 – высокий, для более крупного – средний).

Для определения мер противодействия угрозам в методике предлагаются каталоги средств. В отличие от прочих методик, OCTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OCTAVE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ.

Методика RiskWatch

Компания RiskWatch [8] разработала собственную методику анализа рисков и семейство программных средств, в которых она реализуется. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности: «RiskWatch for Physical Security» для анализа физической защиты ИС; «RiskWatch for Information Systems» для информационных рисков; «HIPAA-WATCH for Healthcare Industry» для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act), актуальных в основном для медицинских учреждений, работающих на территории США; «RiskWatch RW17799 for ISO 17799» для оценки соответствия ИС требованиям международного стандарта ISO 17799.

RiskWatch в качестве критериев для оценки и управления рисками использует ожидаемые годо-

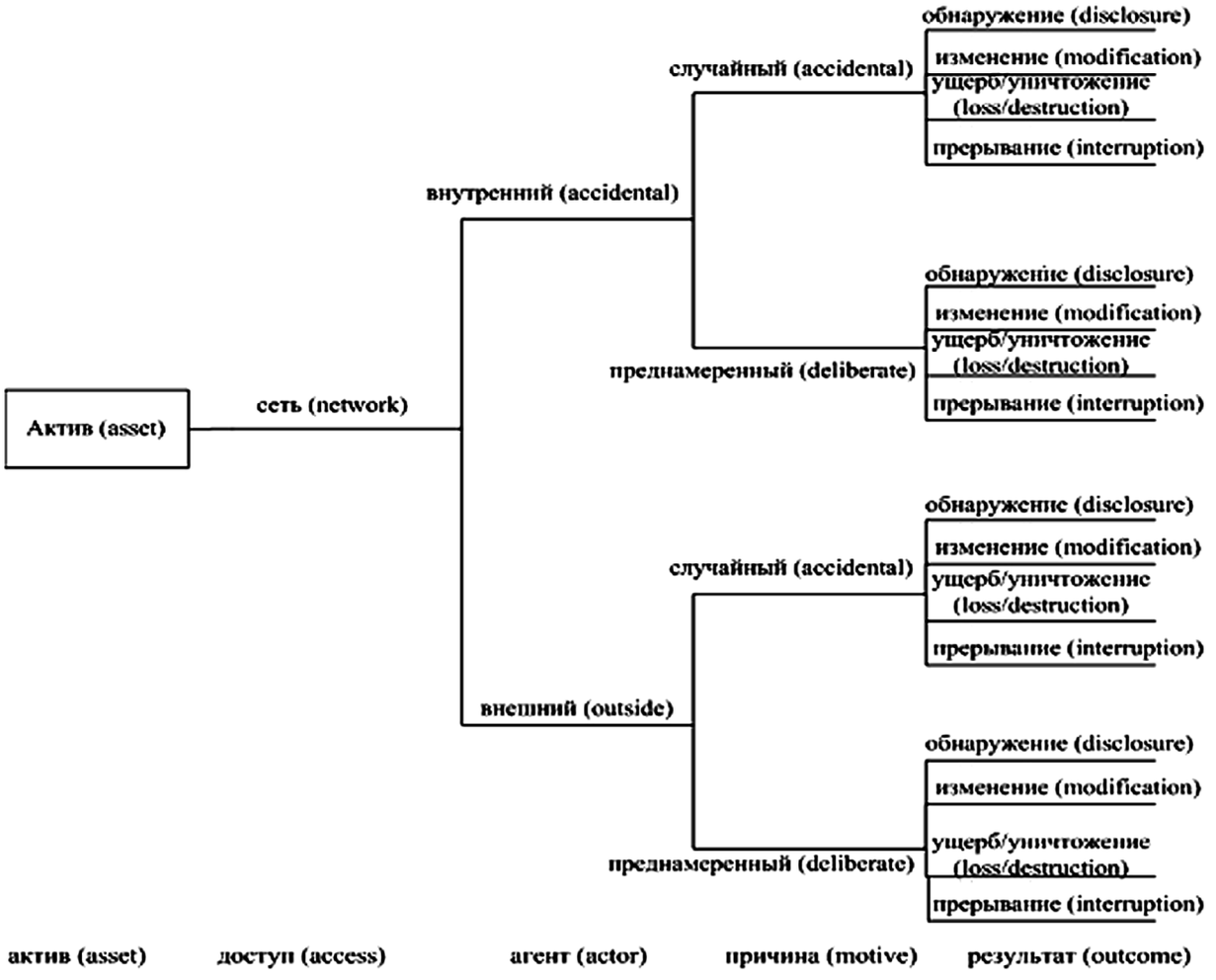

Рис. 2. Дерево вариантов, используемое при описании профиля в методике OCTAVE

вые потери (Annual Loss Expectancy, ALE) и оценку возврата инвестиций (Return on Investment, ROI). Методика RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

На первом этапе определяется предмет исследования. Описываются такие параметры, как тип организации, состав исследуемой, базовые требования в области безопасности. Для облегчения работы аналитика в шаблонах, соответствующих типу организации («коммерческая информационная система», «государственная/военная информационная система» и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Второй этап – ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе подробно описываются ресурсы, потери и классы инцидентов, получаемые путем сопоставления категории потерь и категории ресурсов. На рис. 3 приведено изображение с экрана RiskWatch: определение категории защищенных ресурсов.

Третий этап – количественная оценка риска. Заключается в расчете профиля рисков и выборе меры обеспечения безопасности. Вначале устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. В целом, риск оценивается с помощью математического ожидания потерь за год.

Оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы (ALE) определяется по формуле:

$$ALE = AssetValue \times ExposureFactor \times Frequency,$$

где *Asset Value* – стоимость рассматриваемого актива (данных, программ, аппаратуры и т.д.); Exposure Factor – коэффициент воздействия, который показывает, какая часть (в процентах) от стоимости актива подвергается риску; Frequency – частота возникновения нежелательного события.

Можно ввести показатели «ожидаемая годовая частота происшествия» (Annualized Rate of Occurrence – ARO) и «ожидаемый единичный ущерб» (Single Loss Expectancy – SLE), который может рассчитываться как разница первоначальной стоимости актива и его остаточной стоимости после происшествия. Тогда для отдельно взятого сочетания «угроза – ресурс» применима формула

$$ALE = ARO \times SLE.$$

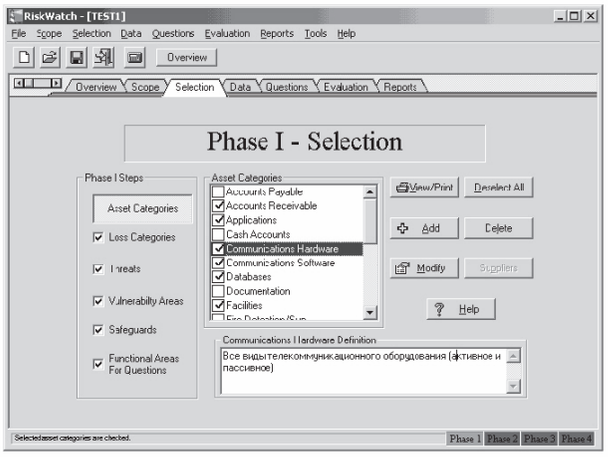

Рис. 3. К определению категории защищенных ресурсов

Эффект от внедрения средств защиты количественно описывается с помощью показателя ROI (Return on Investment – возврат инвестиций), который показывает отдачу от сделанных инвестиций за определенный период времени и рассчитывается по формуле:

$$ROI = \sum_i NVP(Benefits_i) - \sum_j NVP(Costs_j),$$

где $Costs_j$ – затраты на внедрение и поддержание *j*-ой меры защиты; $Benefits_i$ – оценка той пользы (то есть ожидаемого снижения потерь), которую приносит внедрение данной меры защиты; *NPV* (Net Present Value) – чистая текущая стоимость. На четвертом этапе генерируются отчеты.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Заключение

При выборе мер для повышения уровня защиты ИС учитывается одно принципиальное ограничение – стоимость реализации этих мер не должна превышать стоимости защищаемых информационных ресурсов, а также убытков компании от возможного нарушения конфиденциальности, целостности или доступности информации [3].

Современные методы оценки рисков имеют ряд ограничений. Вместе с тем сам рискориентированный подход к управлению ИБ представляется пер-

спективным, в связи с чем необходимо, во-первых, использовать имеющиеся методики в качестве источника информации для принятия решений; во-вторых, совершенствовать методы оценки рисков в направлении преодоления тех ограничений и недостатков, которыми они обладают в настоящее время.

Литература

1. Анализ методов оценки рисков информационной безопасности // http:// igorosa.com/analiz-metodov-ocenki-riskov-informacionnoj-bezopasnosti/
2. Сердюк В. Аудит информационной безопасности. BYTE Россия. №4 (92), 2006 // http://www.bytemag.ru/articles/detail.php?ID=6781
3. Петренко С.А. Возможная методика построения системы информационной безопасности предприятия. security.meganet.md // http://bre.ru/security /13985.html
4. Галатенко В.А. Основы информационной безопасности. // http://www.intuit.ru/ department/ security/secbasics/
5. http://www.peltierassociates.com
6. Software Engineering Institute Carnegie Mellon. OCTAVE // www.cert.org/octave
7. Siemens. The total information security toolkit // http://www.cramm.com
8. Пугин В.В., Губарева О.Ю. Методика Risk Watch для анализа рисков в сфере информационной безопасности // Материалы XIX РНТК ПГУТИ. Самара: 2012. – С. 52.
9. Пугин В.В., Губарева О.Ю. Методика FRAP для анализа рисков в сфере информационной безопасности // Материалы XIX РНТК ПГУТИ. Самара: 2012. – С. 50.

MODERN TECHNIQUES ARE USED TO EVALUATE THREATE AND VULNERABILITIES INFORMATION SYSTEMS

Gubareva O.Yu., Pugin V.V.

Modern information systems trust the solution of the most diverse and important tasks: automatic control of technological processes and industrial enterprises, the automation of activities of banks, financial markets, insurance and trading companies, and so on. Grow the size and complexity of corporate systems. The importance of the task of ensuring the security of corporate information resources is understood as the management of companies, and customers. And already insufficient condition is the organization of the protection of individual segments of the information system. Proceeding from this, the requirements of information security should be aimed at ensuring an optimal regime of functioning of the information system as a whole.

Keywords: *information security, information system, risk, analysis, technique, counter-measure, security, model, audit, threat, vulnerability.*

Губарева Ольга Юрьевна, аспирант Кафедры мультисервисных сетей и информационной безопасности (МСИБ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-927-732-12-11. E-mail: olgagubareva@inbox.ru

Пугин Владимир Владимирович, к.т.н., доцент Кафедры МСИБ ПГУТИ. Тел. 8-927-203-30-00. E-mail: pugin@psati.ru

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 519.876.2.007

МЕХАНИЗМЫ АДАПТИВНОЙ КОРРЕКЦИИ ПРОЦЕССА ПОДГОТОВКИ ВЫСОКОКВАЛИФИЦИРОВАНЫХ ТЕХНИЧЕСКИХ СПЕЦИАЛИСТОВ

Данилаев Д.П., Маливанов Н.Н., Польский Ю.Е.

Статья посвящена анализу условий адаптации процесса подготовки высококвалифицированных технических специалистов требованиям заинтересованных сторон. Показано, что переход к блочно-модульной системе организации учебного процесса позволяет снизить инерционность системы высшего технического образования и обеспечить стабильность взаимодействия ее субъектов.

Ключевые слова: адаптация процесса подготовки, коррекция процесса подготовки, стабилизация системы высшего технического образования, высококвалифицированные технические специалисты

Взаимодействие субъектов системы высшего технического образования (ВТО): государства, работодателя, студента и высшего учебного за-