Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

СПЕЦИАЛИЗИРОВАННЫЕ СИСТЕМЫ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для направления специальности 1-40 05 01-09 «Информационные системы и технологии (в обеспечении промышленной безопасности)»

Минск БГУИР 2016

УДК [331.45+004.56+658-049.5](076.5)
ББК 30.604я73+30ня73
С71

А в т о р ы:
А. Г. Давыдовский, Л. П. Пилиневич, В. В. Савченко, К. Д. Яшин,
М. М. Борисик

Р е ц е н з е н т ы:
кафедра новых материалов и технологий филиала Белорусского национального технического университета «Институт повышения квалификации и переподготовки кадров по новым направлениям развития техники, технологии и экономики БНТУ» (протокол №6 от 23.02.2015);

начальник отдела естественных и технических наук Высшей аттестационной комиссии Республики Беларусь, доктор технических наук, доцент
М. В. Тумилович

Специализированные системы промышленной безопасности : пособие / А. Г. Давыдовский [и др.]. – Минск : БГУИР, 2016. – 68 с. : ил.
ISBN 978-985-543-187-0.

В пособии рассмотрены вопросы анализа современных систем промышленной безопасности. Основное внимание уделено научно-практическим основам современных технологий обеспечения промышленной безопасности. В качестве объекта исследования рассматривается система «человек – машина – среда».

УДК [331.45+004.56+658-049.5](076.5)
ББК 30.604я73+30ня73

ISBN 978-985-543-187-0

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На современном этапе научно-технологического развития общества критически важной проблемой является обеспечение безопасности сложных технологических систем и объектов повышенной опасности (ОПО).

Пособие «Специализированные системы промышленной безопасности» изложено на 68 страницах и содержит 8 лабораторных работ, список рекомендуемой литературы. Лабораторные работы включают теоретическую часть, примеры выполнения и описание порядка выполнения лабораторной работы, варианты заданий для самостоятельной работы и контрольные вопросы. Лабораторные работы посвящены вопросам оценки комплексной характеристики промышленной безопасности; анализу конфигурации охранных инженерно-технических сооружений промышленных объектов; характеристике систем и средств контроля персонального доступа в охраняемые промышленные объекты; интегрированным системам безопасности промышленных объектов; интегрированным интеллектуальным систем обеспечения безопасности транспортных комплексов; системам и средствам профессионального отбора производственного персонала в обеспечении безопасности промышленных объектов; системам и средствам мониторинга функционального состояния производственного персонала; оценке и прогнозированию профессиональной надежности персонала опасных производств.

Содержание пособия соответствует типовому учебному плану направления специальности 1-40 05 01-09 «Информационные системы и технологии (в обеспечении промышленной безопасности)», образовательному стандарту ОСВО 1-40 05 01-2013, квалификационным требованиям к специалисту.

Содержание пособия соответствует уровню подготовленности студентов к изучению новой учебной дисциплины «Специализированные системы промышленной безопасности». При этом успешность освоения практических умений и навыков обеспечивается предшествующей подготовкой студентов по таким дисциплинам, как высшая математика, физика, эргатические системы.

Актуальность и новизна данного пособия обусловлены включением в его содержание важнейших вопросов теории и практического анализа современных средств и систем безопасности промышленных объектов.

Достижения в области развития современных технологий, средств и систем обеспечения безопасности промышленных объектов, технической культуры в области решения задач промышленной безопасности отражены и представлены с использованием системного и социотехнического подхода в соответствии с квалификационными требованиями к подготовке инженера-системотехника.

Лабораторная работа №1

КОМПЛЕКСНАЯ ХАРАКТЕРИСТИКА ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

Цель работы – обеспечить формирование у студентов навыков анализа уязвимости, а также оценки интегрированной комплексной системы безопасности производственного объекта.

Теоретические сведения

Концепция комплексной безопасности производственного объекта (ККБПО) направлена на определение цели и задачи системы безопасности, описание объектов защиты и потенциальных угроз, основных принципов организации и функционирования системы безопасности (СБ), оценки и анализа требований к основным подсистемам безопасности (ПСБ) (рис. 1).

Рис. 1. Структура концепции комплексной безопасности объекта

Каждая из основных подсистем технических средств обеспечения безопасности (ТСОБ) может рассматриваться как интегрированная комплексная система безопасности (ИКСБ), которая отрабатывает свой комплекс угроз и включает в себя совокупность технических средств охраны.

Техническое средство охраны (ТСО) является базовым понятием, обозначающим аппаратуру, используемую в составе комплексов ТСОБ объектов от несанкционированного проникновения.

ТСО – это конструктивно законченное, выполняющее самостоятельные функции устройство, входящее в состав систем охранной, тревожной сигнализации, контроля и управления доступом, охранного телевидения, освещения, оповещения и других систем охраны объекта.

При этом структура комплексной системы безопасности (КСБ) выполняется по классической схеме и состоит из следующих элементов:

1) ССОИУЦ – система сбора и обработки информации и управления центральная – сервер, где хранятся и обрабатываются все базы данных системы; контрольные панели, пульты, консоли управления; в общем случае входит в состав центрального пульта наблюдения наряду с автоматизированными рабочими местами (АРМ) операторов, администраторов систем, постов охраны и службы безопасности;

2) ССОИУП – система сбора и обработки информации и управления периферийная – устройства (контроллеры, расширители, пульты управления), непосредственно на аппаратном уровне взаимодействующие со своими извещателями, датчиками или исполнительными устройствами, а на информационном уровне связывающие их по локальному интерфейсу (RS-485, RS-232) с рабочими станциями или сервером;

3) СОУ – средства обнаружения угроз – извещатели охранной, тревожной, пожарной сигнализации, считыватели, клавиатуры, видеокамеры в зависимости от назначения рассматриваемой КСБ;

4) СПИ – система передачи извещений – каналы и средства передачи служебных и/или тревожных извещений и сообщений, визуальной и акустической информации об объекте и состоянии КСБ;

5) ПО – сетевое, системное и прикладное программное обеспечение сервера и рабочих станций, а также микропрограммное обеспечение системных контроллеров, контрольных панелей и модулей;

6) СБЭП – система гарантированного бесперебойного электропитания, которая включает в себя:

– электрощитовую КСБ, подключенную к сети 220 В и содержащую все необходимые входные и выходные силовые автоматы;

– источники бесперебойного питания (ИБП), обеспечивающие непрерывное и качественное электропитание всей аппаратуры КСБ в течение заданного времени;

– разведенную по всему объекту отдельную сеть питания с размещением при необходимости отдельных ИБП в специально выделенных помещениях, нишах или шкафах, находящихся под охраной;

7) ВУ – вспомогательные устройства, которые обеспечивают выполнение системой охраны ряда функций и включают в себя:

– СО – средства оповещения;

– СОИ – средства отображения информации;

– СРД – средства регистрации данных;

– СПЛУ – средства противодействия и ликвидации угроз.

Безопасность защищаемого производственного объекта – это состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей; имуществу физических или юридических лиц; государственному или муниципальному имуществу; техническому состоянию, инфраструктуре жизнеобеспечения; внешнему виду, интерьеру, ландшафтной архитектуре; окружающей природной среде.

Уязвимость объекта – это степень несоответствия принятых мер по защите объекта прогнозируемым угрозам или заданным требованиям безопасности.

Целями и задачами проведения анализа уязвимости являются:

1) определение важных для жизнедеятельности объекта предметов защиты (наиболее вероятных целей злоумышленных акций нарушителей);

2) определение возможных моделей и угроз вероятных исполнителей угроз (нарушителей);

3) оценка возможного ущерба от реализации прогнозируемых угроз безопасности;

4) оценка уязвимости объекта и существующей системы безопасности;

5) разработка общих рекомендаций по обеспечению безопасности объекта.

Работы по пп. 1–3 проводятся методом экспертных оценок комиссией, в состав которой входят специалисты соответствующих служб заказчика (безопасности, главного технолога, главного инженера, пожарной охраны). Работы по пп. 4 и 5 проводятся с применением методов математического моделирования.

Охраняемый объект – это предприятие, организация, жилище, их часть или комбинация, оборудованные действующей системой охраны и безопасности.

Объект повышенной опасности (ОПО) – объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво-пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения источника чрезвычайной ситуации. В зависимости от категории значимости все объекты, их помещения и территории подразделяются на четыре группы: АI и АII, БI и БII.

Объекты группы АI (особо важные объекты высокой ценности или высокой опасности): 1) объекты особо важные, повышенной опасности и жизнеобеспечения; 2) объекты, включенные органами власти субъектов Республики Беларусь, самоуправления в перечни объектов особо важных, повышенной опасности и жизнеобеспечения; 3) объекты по производству, хранению и реализации наркотических веществ, сильнодействующих ядов и химикатов, токсичных и психотропных веществ и препаратов (базы аптекоуправления, аптеки, склады медрезерва, научные, медицинские и другие учреждения, заведения, в практике которых используются эти вещества);

4) объекты и помещения для хранения оружия и боеприпасов, радиоизотопных веществ и препаратов, предметов старины, искусства и культуры; 5) объекты кредитно-финансовой системы (банки, операционные кассы вне кассового узла, дополнительные офисы, пункты обмена валюты, банкоматы), а также другие аналогичные объекты и имущественные комплексы.

Объекты группы АII (наиболее опасные помещения на объектах группы АI): 1) хранилища и кладовые денежных и валютных средств, ценных бумаг; 2) хранилища ювелирных изделий, драгоценных металлов и камней; 3) хранилища секретной документации, изделий; 4) специальные хранилища взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов; 5) специальные фондохранилища музеев и библиотек.

Объекты группы БI (объекты розничной торговли и пр.): 1) объекты с хранением или размещением изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и другого имущества; 2) объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и другие аналогичные объекты).

Объекты группы БII – объекты категории Б, содержащие алкогольную продукцию с содержанием этилового спирта свыше 13 % объема готовой продукции или наиболее компактные легкосбываемые товары: электронику, товары повседневного спроса.

На рис. 2 показаны элементы комплексной безопасности любого производственного или непроизводственного объекта, включая ОПО.

Рис. 2. Структура системы обеспечения комплексной безопасности объекта

Обобщенная структурная схема ИКСБ представлена на рис. 3.

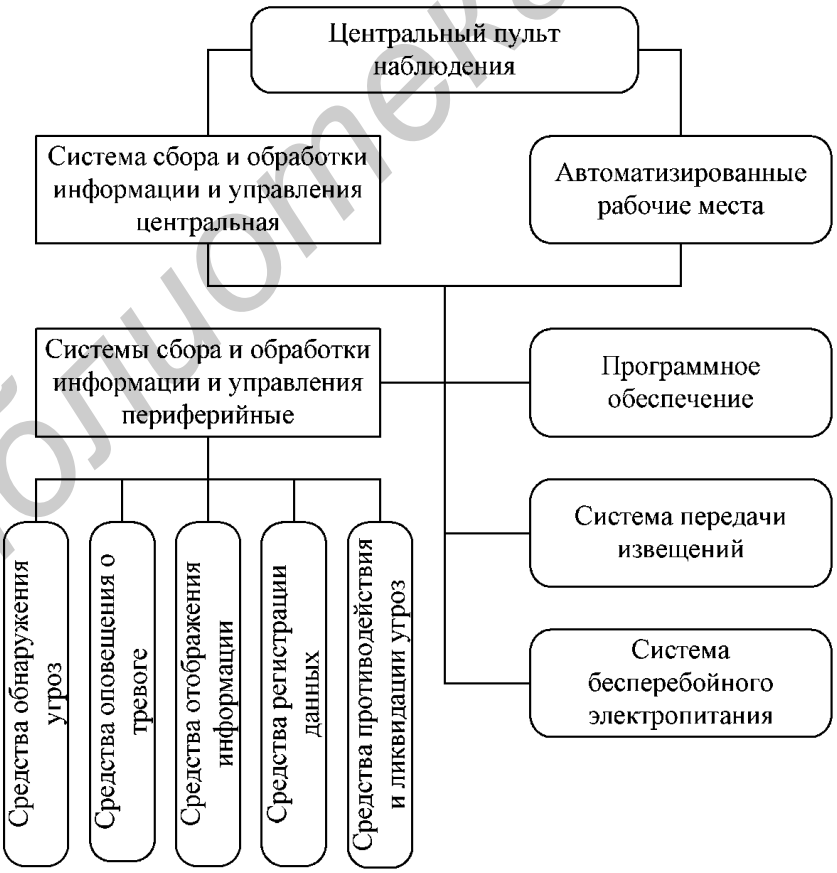

Рис. 3. Обобщенная структурная схема ИКСБ

Эффективность интегрированных комплексных систем безопасности

Определяющими признаками ИКСБ являются:

1) тип информации (сообщения и команды или простейшие аналоговые сигналы), передаваемой между различными ПСБ;

2) схема передачи информации между управляющими устройствами различных подсистем СКУД , в частности, контроллерами, приборами приемно-контрольными (ППК), системами охранной и пожарной сигнализации (ОПС), управляющим и записывающим оборудованием системы охранного телевидения (СОТ);

3) схема принятия решений (централизованная, иерархическая или распределенная);

4) тип управляющих устройств, принимающих решение (контроллеры или компьютеры с установленным программным обеспечением).

При разработке эффективной ИКСБ следует учитывать перспективы развития промышленного объекта, прогноз возникновения новых угроз и современные достижения в области технологий обеспечения промышленной безопасности.

На стадии предпроектного исследования ИКСБ осуществляется анализ уязвимостей на производственном объекте. При этом решаются следующие задачи:

- определение объекта охраны и его категории значимости;
- составление списка и параметров угроз для объекта охраны;
- создание модели нарушителя;
- оценка вероятности реализации угроз;
- оценка потенциального ущерба при реализации угроз;
- оценка эффективности существующей ИКСБ.

По результатам анализа уязвимости разрабатываются общие рекомендации по обеспечению безопасности объекта с ориентировочной оценкой стоимости создания предлагаемой ИКСБ. При этом сравнивается ориентировочная стоимость предотвращаемого ущерба ($С_{ПУ}$) и затраты на создание предлагаемой ИКСБ ($С_{ИСБ}$). Обязательным условием целесообразности внедрения ИКСБ в систему охраны объекта является выполнение неравенства:

$$С_{ПУ} > С_{ИСБ}. \quad (1)$$

С учетом сложности решаемых задач, исходя из принципов рационального и эффективного использования денежных средств, создание системы защиты должно базироваться на следующих принципах:

- разумной достаточности мер;
- четкой правовой основе;
- организованной службе физической охраны;
- оптимальном составе технических средств защиты.

Экономическая эффективность ИКСБ (Э) зависит от использования системы и общих затрат (З), включающих стоимости ее создания и обслуживания в течение срока эксплуатации. При этом оценивается относительная эффективность $Э_о$:

$$Э_О = \frac{П\text{-}З}{П_О} = У_П - \frac{З}{П_О}, \qquad (2)$$

где $П = П_О \cdot У_П$ – упрощенные потери в результате использования системы; $П_О$ – общие возможные потери; $У_П$ – относительный предотвращенный ущерб в результате использования системы безопасности ($0<У_П<1$).

Величина ущерба складывается из следующих составляющих:

– стоимости, направленной на возмещение последствий события (компенсация);

– стоимости похищенного или уничтоженного пожаром имущества, (ремонт объекта и т. п.);

– стоимости дополнительных временных расходов (восстановление работоспособности участка, которому нанесен ущерб);

– относительной стоимости, определенной убытками из-за случившегося хищения или пожара (простой оборудования, штрафы за срыв сроков поставки и т. п.);

– размера материальных затрат и рабочего времени, потраченных на расследование происшествий.

Анализ формулы (2) показывает, что система тем эффективнее ($Э_О>0$), чем выше условный предотвращенный ею ущерб и чем ниже относительные затраты на ее создание и эксплуатацию, т. е. если выполняется соотношение $У_П > З/П_О$.

Пример использования метода оценки экономической эффективности ИКСБ. Пусть стоимость ИКСБ составляет 20 % от суммы возможных потерь, т. е. $С_О = 0{,}2П_О$, срок службы ИКСБ Т=10 лет, затраты на эксплуатацию ИКСБ в течение периода Т составляют 5 % от стоимости системы $С_Э = 0{,}05 \cdot 10С_О$.

Тогда общие затраты на создание системы будут равны:

$$З = С_О + С_Э = 0{,}2П_О + 0{,}05 \cdot 10С_О = (0{,}2 + 0{,}05 \cdot 10 \cdot 0{,}2)П_О = 0{,}3П_О.$$

Таким образом, система будет эффективна, если относительный предотвращенный ущерб $У_п$ составит не менее 30 % общих возможных потерь от реализации угроз.

Необходимо определять влияние каждого элемента ИКСБ на реализацию конкретной угрозы (содействие, независимость, конфликт) для получения значений коэффициентов эффективности каждой ИКСБ.

Комплексный показатель эффективности технических решений ИКСБ можно оценить функциональной зависимостью:

$$К_{ЭФ} = f(k_1, k_2, ..., k_n), \qquad (3)$$

где k_1, k_2, k_3,..., k_N – значения частных показателей эффективности, которые характеризуют основные и вспомогательные подсистемы ИКСБ, включая:

1) надежность оборудования периметра объекта средствами сигнализации;

2) инженерную подготовку местности (подступы к объекту, внешняя полоса отчуждения, внутренняя запретная зона) и периметра;

3) характеристики и параметры ССОИУ;

4) характеристики и параметры СКУД;

5) характеристики и параметры СОТ;

6) характеристики системы тревожного освещения (СТО);

7) характеристики системы оперативной связи (СОС);

8) системы резервного бесперебойного электроснабжения (СЭС), климатической и вандалозащищенности;

9) мероприятия по противодействию технической разведке (ПДТР) организованных преступных групп, незаконных вооруженных формирований и иностранных спецслужб.

При оценке эффективности ИКСБ результативным может быть метод групповой экспертизы, т. к. групповые оценки позволяют компенсировать смещения оценок отдельных членов экспертной группы. Группа экспертов может насчитывать от 3 до 7 специалистов разного профиля. В специальных анкетах эксперты выставляют оценку в баллах по каждому из частных показателей эффективности. После обработки результатов экспертных оценок получают усредненные частные показатели эффективности комплекса ИКСБ по шкале оценок от 1 до 5 (табл. 1).

Таблица 1

Значения частных показателей эффективности подсистем безопасности

Периметр	ССОИУ	Инж. оборуд.	СОТ	СКУД	СЭС	СОС	ПДТР	СТО
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9

Обоснование оптимального выбора ИКСБ выполняется методом обобщенных параметров оптимизации. В методе переходят от абсолютных значений частных показателей, имеющих свой физический смысл и размерность, к безразмерной обобщенной функции желательности Харрингтона (Desirability Profile), которая определяется следующим образом:

$$d = \frac{1}{e^{x\sqrt{e}}}, \qquad (4)$$

где e – основание натурального логарифма; x – приведенное значение исследуемого показателя.

Как показано на рис. 4, функция определена в интервале [0; 1] и используется в качестве безразмерной шкалы, названной шкалой желательности или предпочтительности, для оценки уровней сравниваемых показателей подсистем.

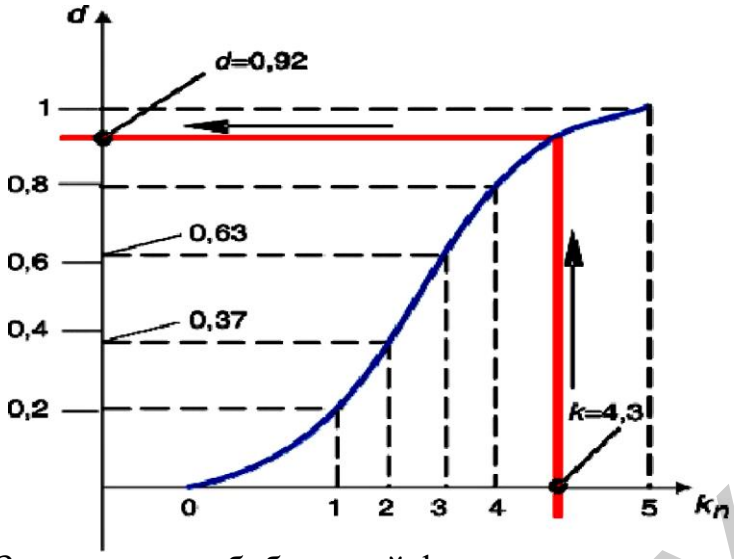

Рис. 4. Зависимость обобщенной функции желательности (d) от частных показателей эффективности ПСБ (k_n)

Шкала желательности устанавливает соотношение между натуральным значением частного показателя (k_n) и значением функции желательности (d). При этом значение d=0 соответствует абсолютно неприемлемому значению частного показателя, а d = 1 – самому лучшему его значению. Искомую обобщенную функцию желательности можно рассматривать как комплексный показатель эффективности $K_{ЭФ}$ согласно формуле

$$K_{ЭФ} = \sqrt[n]{S_1 S_2 S_3 \ldots S_n}, \qquad (5)$$

где $S_n = d_n \cdot g_n$ – значение обобщенного частного показателя эффективности подсистемы с учетом его значимости; d_n – значение функции желательности; g_n – коэффициент значимости подсистемы назначается на основе экспертной оценки и находится в диапазоне от 1 до 10.

Задания для самостоятельного выполнения

Задание 1. Изучить обобщенную структурную организацию КСБ, используя рис. 3. Проанализировать функционирование ИКСБ с помощью «дерева событий» и оценить надежность ее функционирования при следующих условиях: а) все компонентные блоки ИКСБ функционируют надежно с вероятностью P=0,8; б) блок средств обнаружения угроз функционирует надежно с вероятностью P=0,5; в) система оповещения о тревоге функционирует надежно с вероятностью P=0,75; г) система бесперебойного электропитания функционирует надежно с вероятностью P=0,5.

Задание 2. Проанализировать функционирование ИКСБ, представленной на рис. 3, с помощью «дерева событий». Оценить надежность функционирования КСБ при следующих условиях: а) все компонентные блоки ИКСБ функционируют надежно с вероятностью P=0,5; б) блок средств регистрации данных функционирует надежно с вероятностью P=0,75; в) система противодействия и ликвидации угроз функционирует надежно с вероятностью P=0,8; г) система отображения информации функционирует надежно с вероятностью P=0,6.

Задание 3. Стоимость ИКСБ составляет 45 % от суммы возможных потерь, срок службы ИКСБ составляет T=8 лет, затраты на эксплуатацию ИКСБ в течение периода T составляют 12 % от стоимости системы. Рассчитать общие затраты на создание подобной системы.

Задание 4. Стоимость ИКСБ составляет 7 % от суммы возможных потерь, срок службы ИКСБ составляет T=15 лет, затраты на эксплуатацию ИКСБ в течение периода T составляют 18,5 % от стоимости системы. Рассчитать общие затраты на создание подобной системы.

Задание 5. При проектировании ИКСБ промышленного предприятия на основе обобщения экспертных оценок были получены следующие усредненные частные показатели эффективности ПСБ комплекса ИКСБ (табл. 2).

Таблица 2

Показатели компонентов системы промышленной безопасности

Вариант задания	Периметр	ССОИУ	Инж. оборуд.	СОТ	СКУД	СЭС	СОС	ПДТР	СТО
	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9
1	1	3	4	2	4	1	5	3	4
2	4	2	3	1	2	3	5	4	4
3	3	3	2	5	1	5	4	2	3
4	5	5	1	1	2	3	4	2	2
5	1	2	2	1	1	2	2	1	2
6	4	3	2	5	4	2	4	2	4
7	3	2	3	4	5	2	4	5	1
8	5	1	1	5	5	1	1	5	1
9	2	5	1	4	2	5	5	1	4
10	4	1	3	5	2	4	2	5	2

Необходимо выполнить следующее:

1) оценить значения функции желательности;

2) предложить значения коэффициента значимости ПСБ в диапазоне от 1 до 10;

3) рассчитать значения обобщенного частного показателя эффективности ПСБ с учетом его значимости;

4) рассчитать комплексный показатель эффективности $K_{ЭФ}$ для проектируемой ИКСБ.

Варианты заданий для самостоятельной работы

Варианты заданий для самостоятельной работы представлены в табл. 3.

Таблица 3

Варианты заданий для лабораторной работы №1

Варианты	Номера заданий
1	1, 5
2	2, 5
3	3, 5
4	2, 4
5	1, 4
6	3, 4
7	2, 3
8	1, 4
9	3, 5
10	4, 5

Контрольные вопросы

1. Какие задачи решает концепция обеспечения комплексной безопасности производственного объекта?
2. Что такое безопасность защищаемого производственного объекта?
3. Охарактеризуйте цели анализа уязвимости объекта.
4. Что такое объект повышенной опасности?
5. Охарактеризуйте структуру системы обеспечения комплексной безопасности объекта.
6. Опишите структуру ИКСБ.
7. Как осуществляется анализ уязвимостей на производственном объекте на стадии предпроектного исследования ИКСБ?
8. Перечислите характеристики эффективности подсистем безопасности.

Лабораторная работа №2

АНАЛИЗ КОНФИГУРАЦИИ ОХРАННЫХ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СООРУЖЕНИЙ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Цель работы – обеспечить освоение студентами навыков анализа конфигурации охранных инженерно-технических сооружений промышленных объектов.

Теоретические сведения

ИТСОН (инженерно-технические сооружения охраны и надзора) промышленных объектов – это система средств, которые применяются с целью создания условий для предупреждения и пресечения несанкционированного доступа на ОПО, включая режимную территорию и помещения.

Инженерные средства охраны и надзора (ИСОН) предназначены для надежного обеспечения безопасности охраняемого объекта. К ИСОН относятся:

- ограждения объектов охраны;
- инженерные заграждения;
- сооружения и конструкции на постах;
- сооружения и конструкции в специальных (режимных) зданиях и помещениях;
- сооружения и конструкции на КПП;
- сооружения и конструкции на внутренней территории объекта;
- оборудование специальных транспортных средств;
- осветительные установки;
- средства электроснабжения;
- средства инженерного вооружения (СИВ).

Система ИСОН включает: 1) ограждения объектов охраны; 2) инженерные заграждения (устанавливаются в пределах запретных зон, в специальных зданиях, на инженерных коммуникациях и внутри объектов охраны; 3) сооружения и конструкции на постах (наблюдательные вышки, площадки, постовые грибы и будки; тропы нарядов и специалистов ИТО; контрольно-следовые полосы – КСП; разграничительные и контрольные знаки; посты караульных собак; оборонительные сооружения); 4) сооружения и конструкции в специальных (режимных) зданиях и помещениях (двери; замковые и запорные устройства; оконные решетки; решетчатые перегородки; ключеулавливатели); 5) сооружения и конструкции на контрольно-пропускном пункте (КПП) производственного объекта; 6) сооружения и конструкции на внутренней территории объекта; 7) оборудование специальных транспортных средств; 8) средства инженерного вооружения, которые применяются для облегчения изготовления, установки и обслуживания инженерных заграждений и для их мобильного развертывания).

Технические средства охраны и надзора (ТСОН) включают: 1) системы и устройства сбора и обработки информации (комплексы и компьютеризированные системы, концентраторы, системы контроля доступа); 2) средства обнаружения; 3) приборы контроля и досмотра (применяются для обеспечения надлежащего контроля и досмотра людей и транспорта на предмет обнаружения сокрытых запрещенных предметов); 4) средства тревожной сигнализации (сигнализационные средства оповещения; применяются для подачи светового и звукового сигналов о чрезвычайных обстоятельствах на объектах охраны, вызова должностных лиц, а также для сбора сотрудников

учреждения по тревоге); 5) средства оперативной связи; 6) средства видеонаблюдения (применяются для дистанционного наблюдения за обстановкой в охраняемых зонах, на территории объекта, в режимных зданиях и помещениях, на подступах к территории ОПО).

Методика расчета плотности ИТСОН на охраняемых объектах

Надежность охраны объекта зависит от плотности, работоспособности ИТСОН и подготовленности персонала охраны и надзора.

Плотность ИТСОН – это комплексное понятие, которое определяет насыщенность запретной зоны объекта и его внутренней территории инженерными и техническими средствами.

Плотность ИТСОН зависит от:

– тактико-технических характеристик инженерных и технических средств, установленных в запретной зоне и на внутренней территории объекта;

– достоверности подачи сигнала «Тревога» техническими средствами, установленными в запретной зоне и на внутренней территории объекта;

– количества и размещения инженерных и технических средств, установленных в запретной зоне и на внутренней территории объекта.

При условии гарантированной подачи сигнала «Тревога» техническими средствами плотность ИТСОН будет зависеть только от количества, качества и тактико-технических характеристик инженерных средств. Поэтому плотность ИТСОН условно можно измерять в секундах.

Плотность ИТСОН обозначают как $\rho_{ИТСОН}$.

Если $\rho_{ИТСОН}$ = 210 с, то это означает, что инженерно-технические средства охраны гарантируют:

– подачу достоверного сигнала «Тревога» техническими средствами;

– задержание нарушителя инженерными средствами охраны в пределах запретной зоны объекта за время не менее 210 с.

Плотность ИТСОН определяется как сумма значений времени преодоления нарушителем тех элементов ИТСОН запретной зоны, которые установлены после первого рубежа обнаружения:

$$\rho_{ИТСОН} = \sum_{i=1}^{k} T_{\text{пр}(i)}, \qquad (6)$$

где k – количество элементов ИСО запретной зоны, установленных после первого рубежа обнаружения; $T_{\text{пр}(i)}$ – время преодоления нарушителем элемента ИСО.

Очевидно, что время преодоления нарушителем элемента ИСО и время задержание нарушителя элементом ИСО есть одна и та же величина.

Поэтому также правильно будет запись

$$\rho_{ИТСОН} = \sum_{i=1}^{k} T_{\text{зн}(i)}, \qquad (7)$$

где $T_{\text{зн}(i)}$ – время задержания нарушителя элементом ИСО.

Плотность ИТСОН может быть достаточной (или недостаточной) для гарантированного задержания нарушителя резервной группой караула в пределах запретных зон охраняемых объектов. Охрана ОПО может осуществляться выставлением часовых (постовых) или оперативным дежурством караула (наряда). Охрану промышленных объектов с помощью часовых осуществляют такими способами, как наблюдение с оборудованных наблюдательных пунктов и вышек, патрулирование вокруг объекта по установленному маршруту.

При организации охраны объектов часовому в зависимости от характера объекта, степени оборудования его ИТСОН и условий местности назначается для охраны определенный участок полосы: при охране объектов с наблюдательных вышек – до 400 м, способом патрулирования – до 500 м ночью и до 1000 м днем.

Определение плотности ИТСОН на примере разреза периметра представлено на рис. 5.

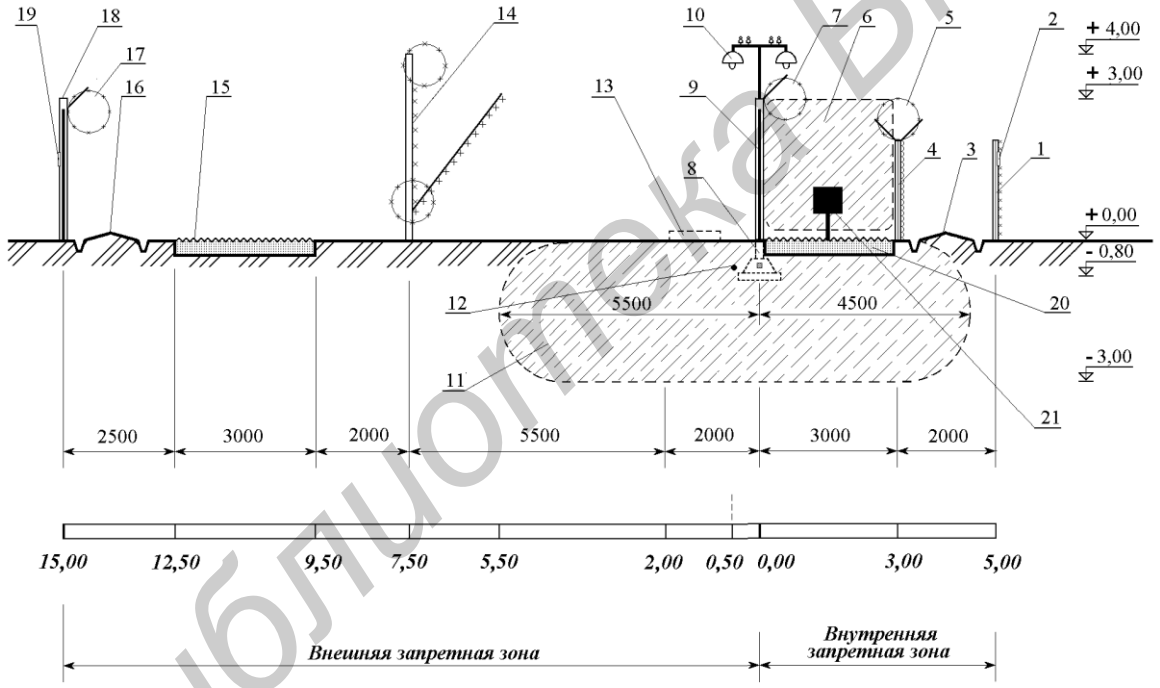

Рис. 5. Порядок определения плотности ИТСОН на ОПО:

1 – ограждение внутренней запретной зоны; 2, 19 – предупредительный знак; 3 – внутренняя тропа наряда; 4 – экранное ограждение рубежа обнаружения; 5, 7, 17 – охранный козырек; 6, 11 – рубеж обнаружения ТСО; 8 – подземное усиление; 9 – основное ограждение; 10 – охранное освещение; 12 – противоподкопный датчик; 13 – тропа специалистов ИТСО; 14 – заграждение «Шиповник-М2-1»; 15, 20 – КСП; 16 – внешняя тропа наряда охраны; 18 – ограждение внешней запретной зоны; 21 – радиолучевое средство двухпозиционное «Редут-300».

Плотность ИТСОН – 108 с.

Порядок определения плотности ИТСО на примере объекта охраны

Предположим, что оборудование периметра обследуемого объекта ИТСО на 12 и 11 участках запретной зоны на удалении 100–200 м от КПП соответствует приведенному на рис. 5. Срок эксплуатации ИСО, установленных на объекте, – 20 лет.

Изделия из армированной колючей ленты и армированной скрученной колючей ленты (АКЛ и АСКЛ) на рассматриваемом участке заменены 3 года назад. Технические средства охраны данного участка обеспечивают гарантированную подачу сигнала «Тревога».

Время пресечения несанкционированного доступа на территорию ОПО определяется инженерными заграждениями и их тактико-техническими характеристиками, количеством, сроком службы и техническим состоянием (табл. 4).

Таблица 4

Время пресечения несанкционированного доступа заграждениями, оборудованными охранными козырьками из спирали АСКЛ

Вид заграждения		Срок службы заграждения, лет	Срок эксплуатации заграждения с момента последнего капремонта, лет									
Заполнение	Высота, м		До 2	2–6	6–12	12–16	16–20	20–30	30–35	35–40	40–45	45–55
			Время преодоления, с, не менее									
Сплошное (железобетон, кирпич)	2,0	45	12	12	10	7	4	3	3	3	3	2
	2,5		17	17	15	12	8	7	7	7	7	5
	3,0		24	24	19	17	11	10	10	10	10	8
	3,5		39	38	24	29	15	14	14	14	13	9
	4,0		50	49	47	35	27	25	25	25	22	18
	4,5		57	54	55	43	38	35	35	35	30	25
	5,0		67	66	65	54	45	40	40	40	36	29
Сплошное (дерево)	2,0	15	12	12	11	10	4	Износ более 80 %				
	2,5		17	17	16	15	6					
	3,0		24	24	23	21	9					
	3,5		39	38	37	34	14					
	4,0		50	49	48	44	18					
	4,5		57	56	55	50	20					
	5,0		67	66	64	59	20					
АСКЛ	2,0	15	16	16	15	14	5	Износ более 80 %				
	2,5		19	19	18	17	7					
	3,0		23	24	22	20	8					
Сетка	2,0	15	8	8	8	7	4	Износ более 80 %				
	2,5		11	11	11	9	6					
	3,0		16	16	15	14	6					
	3,5		25	25	24	21	10					
	4,0		33	33	32	29	12					
	4,5		38	37	36	33	14					
	5,0		38	37	36	33	14					
Колючая проволока	2,0	12,5	10	10	9	5	Износ более 80 %					
	2,5		12	12	11	6						
	3,0		15	15	14	6						

Нарушитель, совершая проникновение на данном участке ОПО, преодолел заграждение внутренней запретной зоны и экранное заграждение. После этого он оказался в зоне рубежа обнаружения, сработал датчик и прозвучал сигнал «Тревога». С этого момента ведем отсчет времени.

Далее нарушитель преодолевает основное заграждение (железобетонное, высотой 3 м) с козырьком из спирали АСКЛ. По табл. 4 определяем, что он затратил на это не менее 24 с.

Преодолев основное ограждение, нарушитель попадает во внешнюю запретную зону. Установленное во внешней запретной зоне защитное заграждение «Шиповник-М2-1» нарушитель преодолевает не менее чем за 60 с.

На преодоление маскировочного ограждения (железобетонное, высотой 3 м) с козырьком из спирали АСКЛ нарушитель затрачивает 24 с.

Следовательно, время преодоления нарушителем запретной зоны объекта на рассматриваемом участке, или, что то же самое, время задержания нарушителя ИСО составляет

$$T_З = 24+60+24=108 \text{ с.}$$

Данные по каждому участку периметра заносятся в таблицу (см. табл. 4). В первом столбце указываются: удаленность от КПП начала и конца участка; во втором – ИСО, которыми оборудован данный участок, и время задержания нарушителя каждым из ИСО; в третьем – суммарное время пресечения несанкционированного доступа путем проникновения на данном участке ОПО.

Контрольные вопросы

1. Охарактеризуйте инженерно-технические сооружения охраны и надзора на производственных объектах.
2. Какие задачи решает система инженерно-технических сооружений охраны и надзора?
3. Классифицируйте инженерно-технические сооружения охраны и надзора на производственных объектах.
4. Перечислите и охарактеризуйте компоненты системы инженерно-технических сооружений охраны и надзора на производственных объектах.
5. Опишите и классифицируйте инженерные средства охраны и надзора.

Лабораторная работа №3

СИСТЕМЫ И СРЕДСТВА КОНТРОЛЯ ПЕРСОНАЛЬНОГО ДОСТУПА В ОХРАНЯЕМЫЕ ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

Цель работы – обеспечить освоение студентами навыков оценки риска причинения ущерба опасным производственным объектам в результате попыток несанкционированного доступа.

Теоретические сведения

Задачи, решаемые СКУД:

– пропуск сотрудников и автотранспорта на охраняемый объект;

– регистрация попыток несанкционированного доступа (ПНД) на ОПО лицами или техническими средствами (автомобилями, автономными наземными, воздушными и иными техническими средствами), а также попыток несанкционированного доступа к информационным ресурсам ОПО;

– блокирование ПНД лицам и техническим средствам на ОПО;

– контроль рабочего времени персонала;

– автоматизация допуска на территорию, разгрузка бюро пропусков от рутинной работы;

– выявление нарушителей пропускного режима;

– многоуровневая идентификация людей и транспорта на пунктах доступа;

– минимизация человеческого фактора при принятии решения о допуске;

– гарантия получения точной и достоверной информации непосредственно руководителем;

– решение управленческих задач по оптимизации производственной деятельности благодаря интеграции системы допуска с автоматизированной системой управления объекта.

Единая система видеонаблюдения крупного ОПО включает несколько сотен видеокамер различного типа, в том числе купольные и мегапиксельные, более 40 видеорегистраторов, объединенных в единую систему с распределенным доступом. Видеомониторинг любого участка предприятия осуществляется с любого автоматизированного рабочего места (АРМ) в соответствии с правами пользователя. Конфигурация оборудования хранится на едином SQL-сервере. Руководитель подразделения/предприятия в соответствии с правами доступа может оперативно загрузить и вывести на монитор видеоинформацию с объекта.

Программное обеспечение СЕКЬЮРИТИ ВИЗАРД (Security Wizard или SW) – основа комплексных систем безопасности от компании «Электроника». Программа позволяет интегрировать все подсистемы безопасности объекта (видеонаблюдение, охрана периметра, контроль доступа, охранно-пожарная сигнализация) в единый комплекс и управлять интегрированной системой через компьютерную сеть.

Внедрение системы позволяет предприятию значительно снизить и практически исключить утрату продукции из-за хищений, использовать ресурсы системы для технологического контроля, анализа и принятия управленческих решений.

Организационный и производственный эффект:

– повышение технологической и трудовой дисциплины;

– эффективность работы службы безопасности;

– повышение ответственности сотрудников за результаты труда;

– оптимизация производственных процессов (отгрузка, логистика и т. д.).

Цели реализации внешних ПНД и внутренних дестабилизирующих явлений, инспирируемых самими пользователями (агентами) в сложных ОПО, разнообразны и могут быть классифицированы в зависимости от преследуемых целей (табл. 5).

Таблица 5

Классификация целей несанкционированного доступа на производственные объекты

Ранг ПНД	Цель атаки или дестабилизирующих действий
10	Создание угрозы национальной безопасности и политической дестабилизации
9	Создание угрозы ядерной, биологической, химической безопасности
8	Возникновение паники и хаоса в обществе
7	Попытки асоциальной и противоправной (преступной) деятельности
6	Получение финансовой выгоды от асоциальной или противоправной (преступной) деятельности
5	Дестабилизация или взятие под контроль (захват) опасных материалов, технологий, технических средств и продукции
4	Несанкционированный доступ к конфиденциальной информации
3	Перехват и изменение информации, программного обеспечения, аппаратных средств и т. д.
2	Блокировка линий передачи данных и/или отключение подсистем
1	Несанкционированное проникновение в ОПО с неизвестными целями и труднопрогнозируемыми последствиями

Деятельность любого ОПО сопровождается возникновением угроз осуществления ПНД. Угроза – потенциальная причина нежелательного инцидента, который может приводить к нанесению информационного, экологического, экономического (материального) и технологического ущерба ОПО. Важным критерием оценки угрозы ПНД является риск причинения информационного, экологического, экономического (материального) и технологического ущерба ОПО.

Порядок расчетов

1. Вероятность эффективной ПНД ($P_{\text{ПНД}}$), вызывающей причинение ущерба ОПО, является отношение числа успешных ПНД, т. е. с достижением цели (полностью или частично), к общему числу зафиксированных попыток ПНД за определенный период можно рассчитать по формуле (8):

$$P_{\text{ПНД}} = \frac{N}{F}, \tag{8}$$

где N – количество успешных ПНД; F – общее количество зафиксированных ПНД в ОПО за рассматриваемый период.

2. Нередко на практике ущерб является функцией некоторой случайной величины – переменной состояния рассматриваемой системы.

Величину ущерба ОПО, обусловленного влиянием всех атак *i*-ранга, можно рассчитать по формуле (9):

$$U_{\text{ПНД}} = M_i \cdot Rang_i \cdot P_i, \quad (9)$$

где M_i – количество лиц, чьим интересам нанесен ущерб в результате ПНД; $Rang_i$ – ранг ПНД; $P_i = \frac{N_i}{F_i}$ – вероятность причинения ущерба, обусловленного ПНД$_i$.

Общий ущерб от всех атак можно оценить как

$$U_{\text{ПНД}} = \sum_{i=1}^{n} \left(M_i \cdot Rang_i \cdot P_i \right). \quad (10)$$

Примеры расчета

В табл. 6 на примере задания 1 представлены данные о ПНД на ОПО.

Необходимо рассчитать:

– вероятность эффективности (успеха) ПНД каждого ранга, вызывающей причинение ущерба ОПО;

– величину ущерба под влиянием атак каждого ранга;

– величину общего ущерба.

Таблица 6

Данные о попытках несанкционированного доступа на опасный производственный объект с различной численностью персонала

Номер задания	Ранг попыток нарушения	Кол-во попыток несанкционированного доступа		Численность персонала, *M*	Вероятность успешного несанкционированного доступа	Величина ущерба
		всего, *N*	с достигнутыми целями, *F*			
Задание 1	10	34	4	11280	0,117647	13270,588
	9	33	0	7347	0	0
	8	27	2	411	0,074074	243,556
	7	22	1	274	0,045455	87,182
	6	48	5	313	0,104167	195,625
	5	7	1	264	0,142857	188,571
	4	15	0	167	0	0
	3	88	3	312	0,034091	31,909
	2	44	1	343	0,022727	15,591
	1	108	4	86	0,037037	3,185

Величина общего ущерба от попыток несанкционированного доступа 14 036,20722.

Задания для самостоятельной работы

В табл. 7 представлены задания для самостоятельного выполнения.

Таблица 7

Данные о попытках несанкционированного доступа на опасный производственный объект с различной численностью персонала

Номер задания	Ранг ПНД	Кол-во попыток несанкционированного доступа		Численность персонала, *M*	Номер задания	Ранг ПНД	Кол-во попыток несанкционированного доступа		Численность персонала, *M*
		всего, *N*	с достигнутыми целями, *F*				всего, *N*	с достигнутыми целями, *F*	
1	2	3	4	5	1	2	3	4	5
Задание 1	10	38	0	97 243	Задание 2	10	14	0	88 424
	9	46	0	21 341		9	17	3	22 162
	8	5	2	7413		8	26	1	6283
	7	12	1	3264		7	32	0	3299
	6	4	0	1282		6	45	0	1345
	5	31	0	633		5	2	0	1351
	4	24	1	297		4	14	3	363
	3	13	3	321		3	11	1	367
	2	9	0	199		2	8	1	388
	1	56	9	62		1	77	4	91
Задание 3	10	19	2	29 431	Задание 4	10	7	1	32 167
	9	23	0	11 278		9	48	0	14 297
	8	52	0	1327		8	34	3	2361
	7	44	3	5356		7	26	1	3423
	6	37	1	1198		6	17	2	2381
	5	26	2	1275		5	32	1	1402
	4	15	1	363		4	25	2	368
	3	23	0	194		3	29	0	273
	2	33	0	348		2	43	0	382
	1	111	9	12		1	68	7	180
Задание 5	10	38	0	97 243	Задание 6	10	14	0	88 424
	9	46	0	21 341		9	17	3	22 162
	8	5	2	7413		8	26	1	6283
	7	12	1	3264		7	32	0	3299
	6	4	0	1282		6	45	0	1345
	5	31	0	633		5	2	0	1351
	4	24	1	297		4	14	3	363
	3	13	3	321		3	11	1	367
	2	9	0	199		2	8	1	388
	1	56	9	62		1	77	4	91

Варианты заданий для самостоятельной работы

Варианты заданий для самостоятельной работы представлены в табл. 8.

Таблица 8

Варианты заданий для лабораторной работы №3

Номер задания	Номера задач
1	1, 4 ,6
2	2, 3, 5
3	3, 4, 6
4	4, 5, 6
5	1, 2, 3
6	1, 3, 5
7	2, 4, 6
8	1, 4, 5
9	2 ,5, 6
10	1, 2, 5
11	2, 4, 5
12	2, 3, 4

Контрольные вопросы

1. Дайте определение понятию «попытка несанкционированного доступа».
2. Объясните классификацию целей несанкционированного доступа на опасные производственные объекты.
3. Чем определяется ранг попытки несанкционированного доступа?
4. Как рассчитать вероятность успешной попытки несанкционированного доступа, которая может достичь своей цели?
5. Как рассчитать величину ущерба от попытки несанкционированного доступа определенного ранга?
6. Как рассчитать величину общего ущерба от всех попыток несанкционированного доступа всех рангов?

Лабораторная работа №4

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Цель работы – овладение студентами теоретическими знаниями и практическими навыками оценки и анализа безопасности информации в социотехнических системах для разработки предложений и тактики по повышению функциональной безопасности опасных производственных объектов.

Теоретические сведения

В настоящее время Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) при участии Британского института стандартов (BSI) разрабатывается и совершенствуется семейство международных стандартов в области управления информационной безопасностью серии 27000. Основным разработчиком международных стандартов серии 27000 является BSI.

Для функционирования ОПО важнейшее значение имеют активы – материальные и нематериальные объекты. К информационным активам относятся сети, базы данных, а также репутация и доверие.

Любой ОПО характеризуется наличием определенных информационных уязвимостей, т. е. слабостей в информационном активе, которые могут являться причинами угроз. В свою очередь угрозы – это потенциальные причины нежелательных событий, которые могут привести к нанесению ущерба активам ОПО. Угрозы могут быть случайными или злонамеренными.

В табл. 9 представлены перечни основных уязвимостей ОПО и угроз в различных областях информационной безопасности, которые могут стать следствием этих уязвимостей.

Таблица 9

Перечень уязвимостей и угроз функциональной и информационной безопасности опасных производственных объектов [1]

Уязвимость	Угроза
Безопасность кадровых ресурсов (ISO/IEC 27002:2005, раздел 8)	
Недостаточное обучение безопасности	Ошибки персонала технической поддержки
Неосведомленность в вопросах безопасности	Ошибки пользователей
Отсутствие механизмов мониторинга	Несанкционированное использование программного обеспечения
Отсутствие политики в области корректного использования средств телекоммуникаций и передачи сообщений	Несанкционированное использование сетевого оборудования
Управление коммуникациями и операциями (ISO/IEC27002:2005, раздел 10)	
Сложный пользовательский интерфейс	Ошибки персонала
Передача или повторное использование средств хранения информации без надлежащей очистки	Несанкционированный доступ
Неадекватный контроль изменений	Сбой системы безопасности

Окончание табл. 9

Уязвимость	Угроза
Неадекватное управление сетью	Перегрузка трафика
Отсутствие процедур резервного копирования	Потеря информации
Отсутствие доказательств отправки или получения сообщения	Уход от ответственности
Отсутствие обновления программного обеспечения, используемого для защиты от вредоносного кода	Вирусная инфекция
Отсутствие разделения обязанностей персонала	Злоупотребление системой (случайное или преднамеренное)
Контроль доступа (ISO/IEC 27002:2005, раздел 11)	
Отсутствие защиты мобильного компьютерного оборудования	Несанкционированный доступ к информации
Отсутствующая или некорректная политика контроля доступа	Несанкционированный доступ к информации, системам или программному обеспечению
Отсутствие «выхода из системы», когда покидается рабочая станция	Использование программного обеспечения неавторизованными пользователями
Отсутствие или проведение в недостаточном объеме тестирования программного обеспечения	Использование программного обеспечения неавторизованными пользователями
Приобретение, разработка и сопровождение информационных систем (ISO/IEC 27002:2005, раздел 12)	
Недостаточная защита криптографических ключей	Раскрытие информации
Несовершенная политика в области использования криптографии	Нарушение законодательства или нормативной базы
Отсутствие проверки обрабатываемых данных	Искажение информации
Плохо документированное программное обеспечение	Ошибки персонала технической поддержки
Непонятные или неполные для разработчиков спецификации	Сбой программного обеспечения
Неконтролируемая загрузка и использование программного обеспечения	Вредоносное программное обеспечение

Матричная методология анализа активов, уязвимостей и угроз ОПО

Эффективным инструментом обеспечения функциональной безопасности ОПО является матричная методология анализа активов, уязвимостей и угроз информационной безопасности. Основной принцип данной методологии

заключается в установлении связей между активами, уязвимостями, угрозами и средствами управления ОПО с помощью набора матриц.

В табл. 10 представлена матрица уязвимости, показывающая связь между активами и уязвимостями в ОПО, матрица угроз в табл. 11 также отображает отношения между уязвимостями и угрозами, а матрица контроля в табл. 12 содержит связи между угрозами и средствами контроля. Значение в каждой ячейке должно показывать уровень отношения между элементом строки и столбца таблицы (например, активом и уязвимостью), определяемой по следующей шкале оценки: 0 – нет воздействия, 1 – слабое воздействие, 3 – умеренное воздействие, 9 – сильное воздействие.

При первоначальном анализе формируются списки активов, уязвимостей, угроз и средств контроля и добавляются в соответствующие таблицы матричного типа. Матрицы заполняются путем добавления данных о связи элемента столбца с элементом строки.

Таблица 10

Матрица уязвимостей, характеризующая связь между активами и уязвимостями

Уязвимости	Активы									
	Торговые секреты	Конфиденциальная информация	Репутация (доверие)	Потерянный доход	Затраты на восстановление	Информация	Аппаратные средства	Программное обеспечение	Обслуживание	Коммуникации
Веб-сервер										
Вычислительный сервер										
Брандмауэр										
Маршрутизатор										
Клиентские узлы										
Базы данных										

Наконец, данные из матрицы уязвимости преобразуются с помощью формулы (11), а затем заносятся в матрицу угроз. Пусть есть m активов, относительная стоимость актива C_j $(j = 1, n)$, c_{ij} – воздействие уязвимости v_i на актив a_j. Тогда совокупное воздействие уязвимости v_i на активы ОПО вычисляется по формуле (11):

$$V_i = \sum_{j=1}^{n} v_{ij} \cdot C_j . \qquad (11)$$

Таблица 11

Матрица угроз, устанавливающая связь между угрозами и уязвимостями

Виды уязвимости	Виды угроз					
	Отказ в обслуживании (DoS)	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Физическое повреждение аппаратных
Торговые секреты						
Конфиденциальная информация						
Репутация (доверие)						
Потерянный доход						
Затраты на восстановление						
Информация						
Аппаратные средства						
Программное обеспечение						
Обслуживание						
Коммуникации						

Пусть имеется m угроз, которые действуют на уязвимости d_{ki} – потенциал повреждения от угрозы при уязвимости V_k. Тогда относительное совокупное воздействие угрозы T_k можно оценить по формуле (12):

$$T_k = \sum_{i=1}^{m} d_{ki} \cdot V_k \ . \qquad (12)$$

Таким же образом данные из матрицы угроз преобразуются с помощью формулы (12) и заносятся в матрицу контроля.

Пусть есть q средств управления и контроля, которые могут смягчить m угроз, а e_k – воздействие средства контроля Z на угрозу T_k. Тогда относительное совокупное воздействие средств управления и контроля Z_q можно оценить по формуле (13):

$$Z_q = \sum_{i=1}^{p} e_k \cdot T_k \, . \qquad (13)$$

В результате формируется матрица контроля, представленная в табл. 12, которая характеризует относительную важность различных средств контроля информационной безопасности.

Таблица 12

Матрица контроля, устанавливающая связь между средствами контроля и угрозами

Средства контроля	Виды угроз					
	Отказ в обслуживании (DoS)	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Физическое повреждение аппаратных средств
Брандмауэр						
Система обнаружения вторжений (IDS)						
Обучение персонала						
DMZ – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных						
Политика безопасности						
Конфигурация архитектуры сети						

Пример анализа уязвимостей и угроз с помощью матричной методологии

Рассмотрим процесс анализа уязвимостей, угроз и средств контроля информационной безопасности некоторой компании «Alpha4Ever» с помощью матричной методологии с позиций социотехнического подхода. Он позволяет осуществлять всесторонний анализ собственных активов, уязвимостей и угроз, порожденных бизнес-процессами.

В табл. 13–15 представлены три матрицы, которые связывают активы с уязвимостями, угрозами и средствами контроля информационной безопасностью в ОПО соответственно. Здесь ранжирование приоритета следующее: 1 – не важный, 2 – минимально важный, 3 – важный, но не ключевой, 4 – важный, но находящийся под воздействием ключевого, 5 – ключевой.

В табл. 13 представлена матрица уязвимостей, связывающая уязвимость системы с воздействиями/активами ОПО. Для построения матрицы была вычислена относительная важность активов/воздействий.

Количественные данные в матрице уязвимостей представлены и отсортированы для того, чтобы определить относительную важность уязвимости. Так как внешние хакеры должны проникнуть через брандмауэр, чтобы получить доступ к конфиденциальной информации, брандмауэр занимает первое место в матрице уязвимости.

Таблица 13

Матрица уязвимостей для компании «Alpha4Ever»

Уязвимости (приоритет)	Активы										
	Контроль информации об экспорте	Репутация (доверие)	IP– контроль/управление	Конфиденциальные данные клиентов	Потерянные продажи/доход	Информационная целостность	Доступность сервисов	Коммуникации	Старые и новые программные средства	Старые и новые аппаратные средства	Приоритет
Брандмауэр	9	9	9	9	3	9	3	9	9	9	5
Передача данных	9	9	9	3	3	9	9	9	9	3	4
База данных	9	3	9	9	9	9	3	3	9	3	4
Архитектура приложений	9	9	9	3	3	3	3	1	9	9	4
Физическая безопасность	9	3	3	9	9	3	3	3	1	9	4
Ошибки конфигурации серверов Интернета	9	1	9	9	1	3	9	3	9	1	3
Ошибки конфигурации серверов Интранета	1	9	9	9	1	3	9	3	9	1	3
Устойчивость паролей	9	9	3	9	1	3	1	3	9	1	3
Клиентские узлы (ПК и ноутбуки)	9	3	9	9	1	3	3	1	3	9	3
Аппаратные средства (веб-сервер, маршрутизатор и др.)	1	3	3	1	1	1	1	1	1	1	3
Ненадежное беспроводное	9	3	9	9	1	3	3	1	1	1	1
Сервисы, основанные на Интернете (VPN)	9	1	3	3	1	1	3	1	3	1	1
Перерыв в подаче энергии	1	1	0	0	3	1	9	3	1	1	1

Совокупные данные об уязвимостях были добавлены к матрице угроз наряду с угрозами, соответствующими уязвимостям. Матрица угроз представлена в табл. 14.

Таблица 14

Матрица угроз для компании «Alpha4Ever»

Виды уязвимости	Виды угроз										
	Социоинженерные атаки (отказ в обслуживании – DoS)	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Вторжения (взламывание паролей)	Отказы сервера	Переполнение буфера	Вымогательство	Физическое повреждение аппаратных средств	Приоритет
Государственные, промышленные и деловые секреты	9	9	9	9	9	9	3	3	9	9	5
Конфиденциальная информация	9	9	3	9	3	9	3	3	9	9	4
Репутация (доверие)	9	9	3	9	3	9	3	3	9	3	4
Потерянный доход	9	9	3	9	9	9	3	3	9	3	4
Затраты на восстановление	9	3	3	9	3	3	3	3	9	9	4
Текстовая информация	9	9	3	9	9	9	1	3	3	3	4
Аппаратные средства	9	9	1	3	1	3	1	1	1	9	3
Программное обеспечение	9	9	0	3	1	3	1	0	1	9	3
Обслуживание	9	3	3	3	1	3	1	1	1	9	3
Коммуникации	3	3	1	3	1	1	3	0	0	3	1

В табл. 15 представлена матрица контроля, в которую были добавлены совокупные данные об угрозах из матрицы угрозы и соответствующие им средства контроля. Относительное воздействие различных средств управления на угрозы было также определено с учетом субъективных суждений экспертов, после чего данные были занесены в таблицу и расположены по приоритетам. Результаты этого анализа и совокупные данные из матриц будут использоваться во время интеграции производственных процессов, бизнес-процессов и для выбора программного обеспечения и аппаратных средств в ОПО.

Таблица 15

Матрица средств контроля для «Alpha4Ever»

Средства контроля	Виды угроз											
	Вторжения (взламывание паролей)	Отказы сервера	Физическое повреждение аппаратных средств	Вымогательство	Внутренние атаки	Отказ в обслуживании	Ошибки пользователей	Воровство компьютеров (ноутбуков, серверов)	Нарушение экспортного контроля	Вредоносный код	Переполнение буфера	Приоритет
Брандмауэр	9	1	1	9	9	9	9	3	3	3	9	1
Система обнаружения вторжений (IDS)	9	3	3	9	1	9	1	3	3	9	9	2
Обучение персонала	9	9	0	3	3	1	9	1	3	1	1	5
DMZ – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных	1	9	1	3	1	3	1	9	1	1	1	9
Политика безопасности	9	1	0	0	3	3	3	1	9	3	9	4
Конфигурация архитектуры сети	3	1	1	9	3	3	3	3	9	3	9	3

Задания для самостоятельного выполнения

Задание 1. Дайте подробное описание структуры и персонала конкретного объекта (автотранспортный узел, железнодорожная станция, электроподстанция, аэропорт, химико-технологический комбинат, калийная добывающая компания). Разработайте рекомендации по анализу и построению модели угроз информационной безопасности данного объекта.

Задание 2. На основании результатов выполнения задания 1 предложите набор рекомендаций для совершенствования системы защиты информации предприятия

Задание 3. Эксперты научно-промышленной компании осуществляют испытания новой системы поддержки принятия решений в управлении информационной безопасностью ОПО (рис. 6).

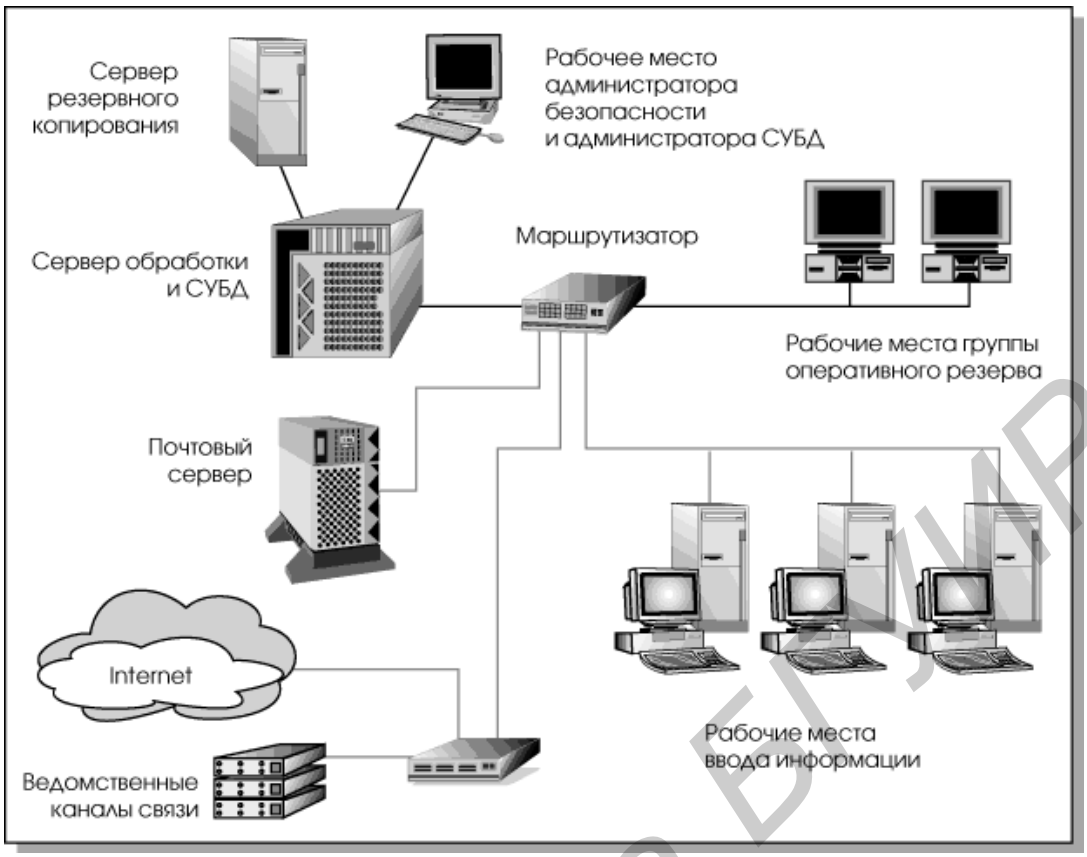

Рис. 6. Система поддержки принятия решений в управлении ОПО

Информация, введенная с рабочих мест и поступившая на почтовый сервер, направляется на сервер обработки. Затем она поступает на рабочие места группы оперативного реагирования, которая принимает решения.

Приведите перечень мероприятий, которые обязаны реализовать эксперты промышленно-финансовой компании для обеспечения защиты информации в этой системе с одновременным ее профильным коммерческим применением.

Задание 4. Международный ядерно-химический концерн «NND» (NasNeDogonysh) предоставляет услуги по обогащению урана-235. Его генеральный директор получил в качестве информационного приложения к контракту с заказчиком проект системы мероприятий по обеспечению промышленной безопасности добывающих и обогатительных предприятий концерна.

Объясните, какие технические решения и мероприятия должны быть предусмотрены в этом проекте.

Задание 5. Разработайте рекомендации по повышению промышленной компании «NND».

Оцените эффективность своих рекомендаций на основе матричной методологии.

Контрольные вопросы

1. Какие составляющие включает информационная безопасность ОПО?
2. Охарактеризуйте смысл матричной методологии анализа активов, уязвимостей и угроз информационной безопасности ОПО.
3. Охарактеризуйте матрицу уязвимостей ОПО.
4. Охарактеризуйте матрицу угроз ОПО.
5. Охарактеризуйте матрицу средств контроля ОПО.

Лабораторная работа №5

ИНТЕГРИРОВАННЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ КОМПЛЕКСОВ

Цель работы – обеспечить освоение студентами навыков анализа и проектирования интегрированных интеллектуальных систем обеспечения безопасности транспортных комплексов с учетом особенностей сетевой топологии транспортных потоков.

Теоретические сведения

Интеллектуальная транспортная система (ИТС, англ. Intelligent transportation system) – это интеллектуальная система, использующая инновационные разработки в моделировании транспортных систем и регулировании транспортных потоков. Согласно директиве «2010/40/EU of 7 July 2010» в странах Евросоюза ИТС рассматриваются как системы, в которых применяются информационные и коммуникационные технологии в сфере автотранспорта (включая инфраструктуру, транспортные средства, участников системы, а также дорожно-транспортное регулирование) и взаимодействующую с другими видами транспорта (подземным, наземным, авиационным, водным и т. д.). Современные ИТС используют системы распознавания автомобильных номеров и регистрации скорости транспортных средств, а также системы интеграции информационных потоков из большого количества различных источников, включая системы управления парковками (Parking guidance and information (PGI) systems), метеослужбы, системы разведения мостов и др. Более того, в ИТС могут применяться технологии прогнозирования на основе моделирования и анализа ранее накопленной информации. В ИТС используются различные виды связи по технологиям WiMAX, GSM, 3G или 4G, по стандартам IEEE 802.11 (Wi-Fi), IEEE802.11p (WAVE), а также по стандарту DSRC (США). Основу интегрированных интеллектуальных систем обеспечения безопасности транспортного комплекса (ИСОБТК) составляют методы анализа сетевой топологии транспортных потоков. Для выбора оптимального варианта интегрированной ИСОБТК (в

масштабах производственного участка, предприятия, мегаполиса, промышленного региона) может быть использован метод анализа иерархий (МАИ), позволяющий осуществлять многофакторную оценку всех вариантов локальных сегментов ИСОБТК на основе следующих критериев:

– безопасность дорожного движения;
– интенсивность (плотность) транспортного потока;
– максимально допустимая скорость движения в транспортном потоке;
– функциональная надежность (риск образования «пробок» и вынужденных остановок и возможные потери в связи с этим);
– стоимость эксплуатации;
– масштабируемость (возможность увеличения размера в будущем);
– удобство организации.

Суть МАИ заключается в иерархической декомпозиции исходной проблемы на все более простые составляющие части и последующем экспертном сравнении этих частей для определения приоритетности имеющихся альтернатив.

Первым этапом применения МАИ является структурирование проблемы выбора в виде иерархии или сети. В вершине иерархии, используемой в МАИ, располагается основная цель, далее, со второго по предпоследний уровень, – подцели, и, наконец, на самом нижнем уровне – альтернативы, среди которых производится выбор. Цель, подцели и альтернативы обычно называют *объектами*, или *элементами иерархии*.

На ***втором этапе*** применения МАИ выясняется интенсивность взаимодействия элементов иерархии. Определение интенсивности взаимодействия позволяет вычислить величину воздействия низших уровней иерархии на высшие уровни и тем самым решить задачу выбора наилучшей альтернативы. Все элементы иерархии одного уровня сравниваются попарно с точки зрения их важности и влияния на принятие решения. Данные суждения выражаются в целых числах с учетом девятибалльной шкалы (табл. 16).

Таблица 16

Шкала для попарного сравнения факторов в иерархии с помощью МАИ

Степень значимости	Объяснение
1	Оба фактора вносят одинаковый вклад в достижение цели
3	Существуют соображения в пользу предпочтения одного из факторов, однако эти соображения недостаточно убедительны
5	Имеются надежные данные или логические суждения для того, чтобы показать предпочтительность одного из факторов
7	Убедительное свидетельство в пользу одного фактора перед другим
9	Свидетельства в пользу предпочтения одного фактора другому в высшей степени убедительны
2, 4, 6, 8	Ситуация, когда необходимо компромиссное решение между влиянием обоих факторов

Эта шкала была разработана на основе междисциплинарных математических, статистических, психофизиологических исследований. Для получения хороших результатов в сравнениях требуется использовать подходящую (универсальную) численную шкалу сравнений и определять степень несогласованности наших суждений. Число сравниваемых объектов должно быть достаточно мало: 7 ± 2. При большем числе сравниваемых объектов на практике можно использовать способ группировки этих объектов в соответствующие классы. Это придает структуре иерархии большую наглядность и облегчает проведение парных сравнений элементов иерархии.

Результаты попарного сравнения элементов заносятся в *матрицу сравнения* размерностью $n \times n$, где n – число сравниваемых элементов. Элемент $a_{ij} = a(i, j)$ указанной матрицы выражает результат сравнения элементов i и j. Если при сравнении элементов i и j получено $a(i, j)=b$, то результатом сравнения элементов j и i должно быть $a(j, i)=1/b$. Очевидно, что диагональные элементы матрицы равны 1. Сравнение элементов проводится на всех уровнях иерархии, начиная со второго. В случае выбора оптимального варианта интегрированной ИСОБТК сначала проводится сравнение авторитетности мнений экспертов, участвующих в принятии решений. После этого каждый эксперт должен, во-первых, провести попарное сравнение важности используемых критериев оценки, а затем выполнить попарное сравнение имеющихся альтернатив с точки зрения каждого из критериев. Количество матриц сравнения для рассматриваемой задачи: $1 + m \cdot (1+8) = 1 + 9 \cdot m$, где m – количество участвующих экспертов.

На третьем этапе происходит обработка полученных данных и синтез вектора приоритетов, который ранжирует рассматриваемые альтернативы с точки зрения их предпочтительности. Для этого прежде всего находят *векторы локальных приоритетов* для каждой из полученных матриц сравнения. Искомый вектор локальных приоритетов w будет равен собственному вектору для максимального собственного значения соответствующей матрицы, нормализованному к единице. Т. Саати предложил упрощенную процедуру вычисления вектора w. Пусть v – вектор *геометрических средних* строк некоторой матрицы сравнения:

$$v = \begin{bmatrix} \sqrt[n]{a(1,1) \cdot \ldots \cdot a(1,n)} \\ \ldots \\ \sqrt[n]{a(n,1) \cdot \ldots \cdot a(n,n)} \end{bmatrix}. \qquad (14)$$

Тогда вектор w будет определяться следующим образом:

$$w = \begin{bmatrix} \dfrac{v_1}{\sum_{i=1}^{n} v_n} \\ \dots \\ \dfrac{v_n}{\sum_{i=1}^{n} v_n} \end{bmatrix}, \qquad (15)$$

где $v_1,\ldots,v_n$ – элементы вектора v.

Пример выбора с помощью метода анализа иерархий

Рассмотрим пример использования метода анализа иерархий для принятия решений. Пусть задача принятия решения состоит в выборе наиболее эффективного проекта интегрированной ИСОБТК.

На рис. 7 представлены элементы иерархии процесса выбора наиболее оптимального проекта ИСОБТК по уровням, которые можно охарактеризовать следующим образом:

1-й уровень (уровень альтернатив): представлены возможные альтернативные проекты построения ИСОБТК: $В_1$, … , $В_4$;

2-й уровень (уровень критериев выбора): представлены наборы критериев оценки функционирования ИСОБТК: $К_1$ – социально-антропологические характеристики, $К_2$ – информационно-технологические характеристики, $К_3$ – характеристики среды;

3-й уровень (акторы, или участники процесса): представлены специалисты (акторы): $Э_1$ – эксперт по промышленной безопасности, $Э_2$ – эксперт по управлению персоналом, $Э_3$ – эксперт по информационно-коммуникационным технологиям;

4-й уровень: принятие решения (ПР) – фокус иерархии, т. е. фокус иерархии соответствует процедуре принятия решения (ПР) по выбору варианта проекта построения ИСОБТК.

Математический аппарат МАИ позволяет получать объективные количественные оценки весомости всех элементов в структуре иерархии на основе исходной информации, связанной с поставленной проблемой.

Представленная на рис. 7 иерархия является примером четырехуровневой неполной иерархии. Иерархия называется *полной*, если между элементами соседних уровней имеются все возможные связи. Если хотя бы одна связь отсутствует, то иерархия называется *неполной*. При этом неполные иерархии всегда можно представить в виде некоторой совокупности полных иерархий, что позволяет разбивать исходную сложную проблему на соответствующую последовательность более простых, четко поставленных задач.

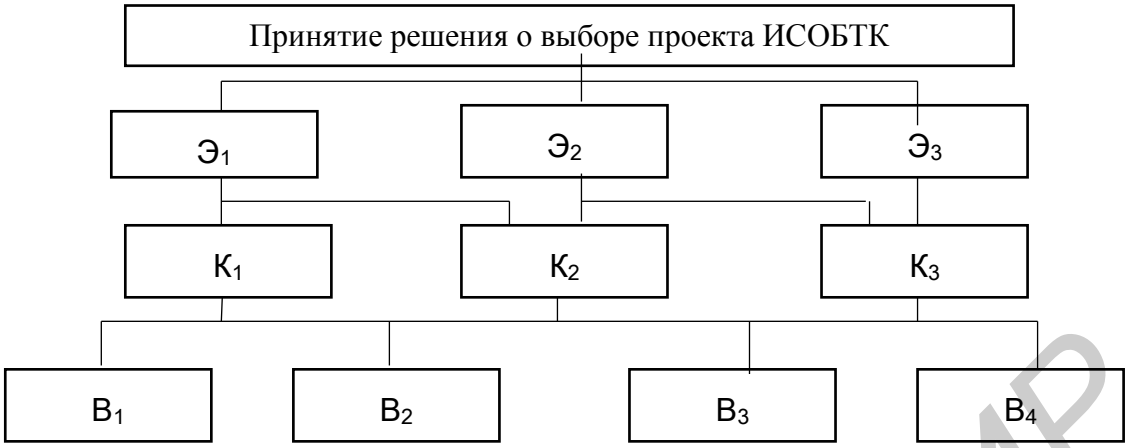

Рис. 7. Иерархическая модель проблемы выбора варианта ИСОБТК

Представленную на рис. 7 неполную четырехуровневую иерархию можно разбить на следующую совокупность трехуровневых полных иерархий, которые моделируют основные этапы работы по выбору варианта проекта построения ИСОБТК. Пусть действия экспертов характеризуются тем, что для эксперта $Э_1$ наиболее приоритетными являются критерии №1 и №2, для $Э_2$ – критерии №2 и №3, а для $Э_3$ – критерий №3. При этом могут быть сформированы полные иерархии для каждого эксперта (рис. 8, 9 и 10).

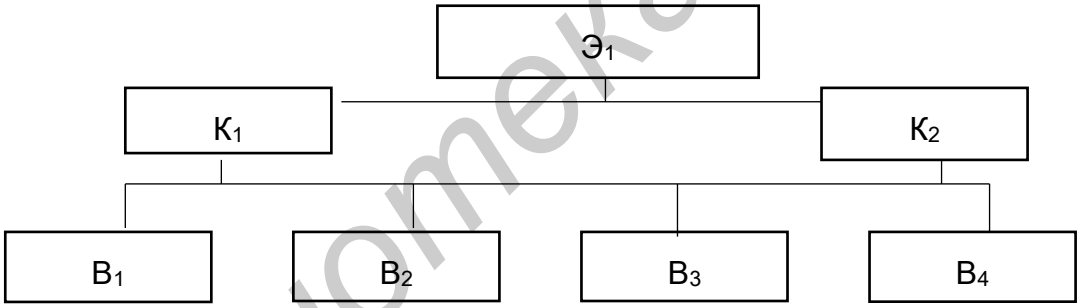

Рис. 8. Полная трехуровневая иерархия для эксперта №1

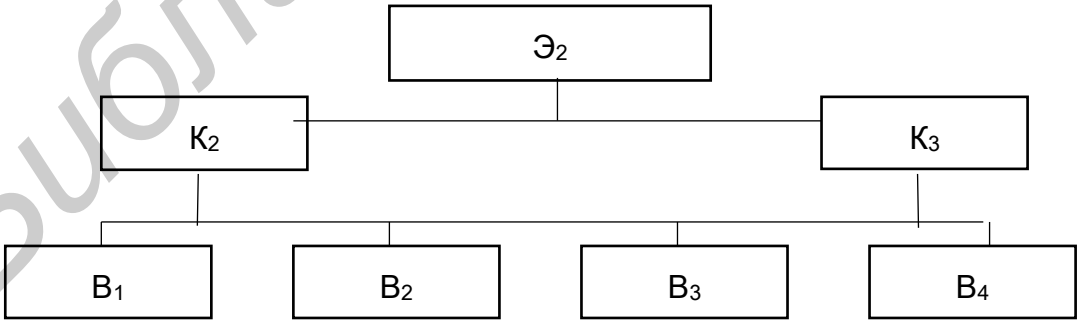

Рис. 9. Полная трехуровневая иерархия для эксперта №2

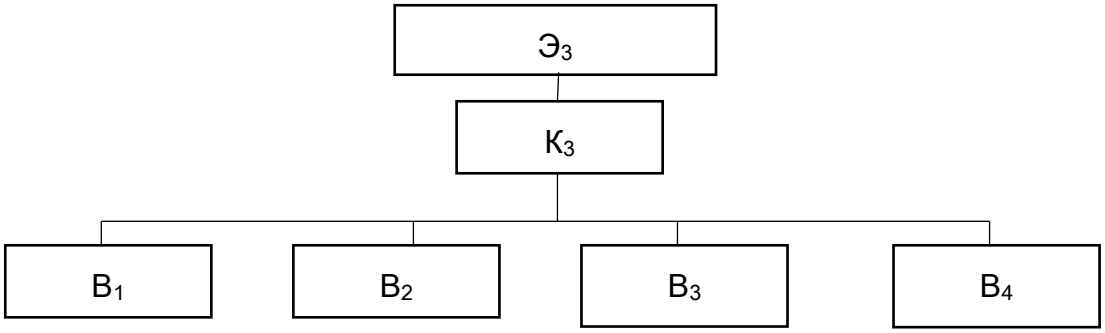

Рис. 10. Полная трехуровневая иерархия для эксперта №3

Этап обсуждения и выбора наиболее эффективного варианта проекта ИСОБТК с помощью группы экспертов и принятие окончательного решения с учетом весомости (квалификации) каждого эксперта моделируется следующей полной двухуровневой иерархией (рис.11):

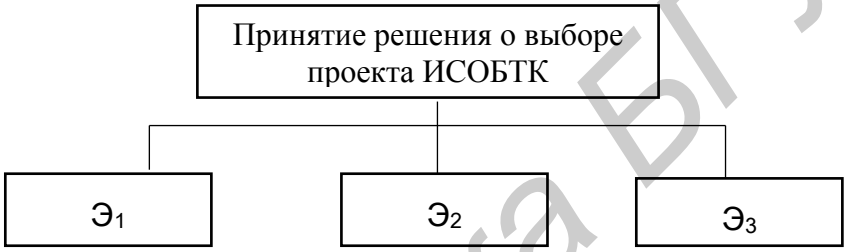

Рис. 11. Полная двухуровневая иерархия для разработки итогового принятия решения о выборе варианта построения ИСОБТК группой экспертов

Парные сравнения для элементов различных уровней иерархии

Приведем один из способов того, как практически придать количественное наполнение сравнению объектов, действий или обстоятельств и построить соответствующую таблицу сравнений. Пусть даны объекты *A*, *B*, *C*, которые образуют матрицу парных сравнений этих объектов по критерию Кр (табл. 17).

Таблица 17

Матрица результатов парных сравнений в общем виде

Кр	*A*	*B*	*C*
A	1	a_{12}	a_{13}
B	$1/a_{12}$	1	$1/a_{23}$
C	$1/a_{13}$	$1/a_{23}$	1

Элементы такой матрицы (a_j определяются по указанным выше правилам, использующим степени предпочтения при сравнении объектов по заданному

критерию, например, в позицию (*A*, *B*) матрицы сравнений ставится число a_{12}, величина которого выбирается из следующих соображений:

– если *A* и *B* одинаково важны (равенство объектов), то ставится число 1;

– если *A* имеет предпочтение над *B* – число 3;

– если *A* имеет выраженное предпочтение над *B* – число 5;

– если *A* имеет сильное предпочтение над *B* – число 7;

– если *A* имеет абсолютно предпочтительнее над *B* – число 9.

Числа 2, 4, 6 и 8 используются для облегчения компромиссов между оценками, слегка отличающимися от основных чисел.

В табл. 18 представлен возможный вариант матрицы парных сравнений элементов B_1, B_2, B_3, B_4 (альтернатив иерархии для проблемы) полученной по критерию K_1. Причем альтернатива B_1 по критерию K_1 предпочтительнее B_2, равна B_3 и уступает (с выраженным предпочтением) альтернативе B_4. Аналогично поясняются остальные строки матрицы.

Таблица 18

Пример матрицы парных сравнений альтернатив по критерию K_1

K_1	B_1	B_2	B_3	B_4
B_1	1	3	1	1/5
B_2	1/3	1	1/3	1/7
B_3	1	3	1	1/5
B_4	5	7	5	1

Далее можно использовать простой алгоритм расчета нормированных весов альтернатив (B_1–B_4) по критерию K_1 на основе матрицы парных сравнений (табл. 18), который включает три шага:

1) вычислить для каждой строки матрицы (для каждой альтернативы) сумму элементов. Обозначим эти суммы соответственно: S_1, S_2, S_3, S_4;

2) вычислить общую сумму: $S = S_1 + S_2 + S_3 + S_4$;

3) вычислить нормированные веса: $W_1 = S_1/S$; $W_2 = S_2/S$; $W_3 = S_3/S$; $W_4 = S_4/S$ для рассматриваемых элементов иерархии.

В соответствии с алгоритмом расчета можно рассчитать суммы для каждой строки матрицы (табл. 18):

1) $S_1 = 1+3+1+1/5 = 5{,}2$;
   $S_2 = 1/3+1+1/3+1/7 = 1{,}81$;
   $S_3 = 1+3+1+1/5 = 5{,}2$;
   $S_4 = 5+7+5+1 = 18$;
2) $S = 5{,}2+1{,}81+5{,}2+18 = 30{,}21$;
3) $W_1=5{,}2/30{,}21=0{,}17$;
   $W_2=1{,}81/30{,}21=0{,}06$;
   $W_3=5{,}2/30{,}21=0{,}17$;
   $W_4=18/30{,}21=0{,}60$.

Приведенный алгоритм является универсальным, т. е. может быть использован для обработки матриц парных сравнений любого размера и позволяет получить нормированные веса сравниваемых объектов с точностью 0,01. При этом сумма нормированных весов: $W_1+W_2+W_3+W_4=1$.

В табл. 19–22 представлены примеры возможных матриц парных сравнений по критериям $К_2$ и $К_3$. В соответствии с рассматриваемой иерархией (рис. 7) по критерию $К_2$ возникает матрица парных сравнений как для эксперта $Э_1$, так и для эксперта $Э_2$. Аналогично по критерию $К_3$ возникает матрица парных сравнений как для эксперта $Э_2$, так и для эксперта $Э_3$. Поэтому для различения таких матриц целесообразно пользоваться, например, критериями: $К_2/Э_1$ и $К_2/Э_2$. Это означает использование критерия $К_2$ экспертом $Э_1$ и, соответственно, использование критерия $К_2$ экспертом $Э_2$.

Таблица 19

Матрица парных сравнений по критерию $К_2/Э_1$

$К_2/Э_1$	$В_1$	$В_2$	$В_3$	$В_4$
$В_1$	1	1/5	1	1
$В_2$	5	1	5	5
$В_3$	1	1/5	1	1
$В_4$	1	1/5	1	1

Таблица 20

Матрица парных сравнений по критерию $К_2/Э_2$

$К_2/Э_2$	$В_1$	$В_2$	$В_3$	$В_4$
$В_1$	1	1	1	1
$В_2$	1	1	1	1
$В_3$	1	1	1	1
$В_4$	1	1	1	1

Таблица 21

Матрица парных сравнений по критерию $К_3/Э_2$

$К_3/Э_2$	$В_1$	$В_2$	$В_3$	$В_4$
$В_1$	1	1	1/5	1
$В_2$	1	1	1/5	1
$В_3$	5	5	1	5
$В_4$	1	1	1/5	1

Таблица 22

Матрица парных сравнений по критерию $К_3/Э_3$

$К_3/Э_3$	$В_1$	$В_2$	$В_3$	$В_4$
$В_1$	1	1	3	1
$В_2$	1	1	3	1
$В_3$	1/3	1/3	1	1/3
$В_4$	1	1	3	1

Выполняя расчеты по указанному выше алгоритму, можно получить нормированные веса альтернатив по критериям для каждого эксперта (табл. 23–25).

Таблица 23

Нормированные веса альтернатив по критериям для $Э_1$

$Э_1$	$В_1$	$В_2$	$В_3$	$В_4$
$К_1/Э_1$	0,17	0,06	0,17	0,60
$К_2/Э_1$	0,125	0,625	0,125	0,125

Таблица 24

Нормированные веса альтернатив по критериям для $Э_2$

$Э_2$	$В_1$	$В_2$	$В_3$	$В_4$
$К_2/Э_2$	0,25	0,25	0,25	0,25
$К_3/Э_2$	0,125	0,125	0,625	0,125

Таблица 25

Нормированные веса альтернатив по критерию для $Э_3$

$Э_3$	$В_1$	$В_2$	$В_3$	$В_4$
$К_3/Э_3$	0,3	0,3	0,1	0,3

Для получения нормированных весов альтернатив на уровне экспертов $Э_1$ и $Э_2$ необходимо знать весомость критериев. Очевидно, каждый эксперт выполняет парные сравнения своих критериев (табл. 26, 27):

Таблица 26

Матрица парных сравнений критериев для $Э_1$

$Э_1$	$К_1$	$К_2$
$К_1$	1	5
$К_2$	1/5	1

Таблица 27

Матрица парных сравнений критериев для $Э_2$

$Э_2$	$К_2$	$К_3$
$К_2$	1	1/5
$К_3$	5	1

На основе этих матриц получают нормированные веса критериев для экспертов $Э_1$ и $Э_2$ (табл. 28, 29):

Таблица 28

Веса критериев для $Э_1$

$Э_1$	$К_1$	$К_2$
Вес (W)	0,83	0,17

Таблица 29

Веса критериев для $Э_2$

$Э_2$	$К_2$	$К_3$
Вес (W)	0,17	0,83

Теперь вычисляют интегрированные веса альтернатив для экспертов $Э_1$ и $Э_2$ на основе результатов, приведенных в табл. 23, 28 для $Э_1$ и табл. 24, 29 для $Э_2$.

Для эксперта $Э_1$ получают следующие интегрированные веса:

$$\begin{aligned} W_{В_1/Э_1} &= 0{,}17\cdot 0{,}83+0{,}125\cdot 0{,}17 = 0{,}162;\\ W_{В_2/Э_1} &= 0{,}06\cdot 0{,}83+0{,}625\cdot 0{,}17 = 0{,}156;\\ W_{В_3/Э_1} &= 0{,}17\cdot 0{,}83+0{,}125\cdot 0{,}17 = 0{,}162;\\ W_{В_4/Э_1} &= 0{,}60\cdot 0{,}83+0{,}125\cdot 0{,}17 = 0{,}520. \end{aligned} \qquad (16)$$

Этот результат (значение весов альтернатив для $Э_1$) соответствует расчету весов в рамках трехуровневой полной иерархии (см. рис. 8)

Аналогично для эксперта $Э_2$ получают следующие интегрированные веса:

$$\begin{aligned} W_{В_1/Э_2} &= 0{,}25\cdot 0{,}17+0{,}125\cdot 0{,}83 = 0{,}14;\\ W_{В_2/Э_2} &= 0{,}25\cdot 0{,}17+0{,}125\cdot 0{,}83 = 0{,}146;\\ W_{В_3/Э_2} &= 0{,}25\cdot 0{,}17+0{,}625\cdot 0{,}83 = 0{,}562;\\ W_{В_4/Э_2} &= 0{,}25\cdot 0{,}17+0{,}125\cdot 0{,}83 = 0{,}146. \end{aligned} \qquad (17)$$

Этот результат (значение весов альтернатив для $Э_2$) соответствует расчету весов в рамках трехуровневой полной иерархии (см. рис. 9).

Для эксперта $Э_3$ уже получены следующие веса (по одному критерию $К_3$) и их нужно просто переписать из табл. 25:

$$\begin{aligned} W_{В_1/Э_3} &= 0{,}3;\\ W_{В_2/Э_3} &= 0{,}3;\\ W_{В_3/Э_3} &= 0{,}1;\\ W_{В_4/Э_3} &= 0{,}3. \end{aligned} \qquad (18)$$

Расчет значений весов альтернатив для $Э_3$ соответствует трехуровневой полной иерархии (см. рис. 10).

Окончательный результат – значения нормированных весов альтернатив в рамках исходной четырехуровневой неполной иерархии (см. рис. 7) может быть получен на основе частных результатов (16–19), если известны веса (уровень квалификации) экспертов (табл. 30):

Таблица 30

Матрица парных сравнений специалистов-экспертов

ПР	$Э_1$	$Э_2$	$Э_3$
$Э_1$	1	1	5
$Э_2$	1	1	5
$Э_3$	1/5	1/5	1

Выполнение расчетов на основе табл. 30 по указанному выше алгоритму позволяет получить нормированные веса для каждого из трех экспертов:

$$W_{Э_1} = 0{,}455;$$
$$W_{Э_2} = 0{,}455; \qquad (19)$$
$$W_{Э_3} = 0{,}090.$$

С учетом полученных результатов (16)–(19) можно рассчитать окончательные значения нормированных весов альтернатив выбора проекта:

$$W_{B_1} = 0{,}162 \cdot 0{,}455 + 0{,}146 \cdot 0{,}455 + 0{,}3 \cdot 0{,}090 = 0{,}167;$$
$$W_{B_2} = 0{,}156 \cdot 0{,}455 + 0{,}146 \cdot 0{,}455 + 0{,}3 \cdot 0{,}090 = 0{,}164; \qquad (20)$$
$$W_{B_3} = 0{,}162 \cdot 0{,}455 + 0{,}562 \cdot 0{,}455 + 0{,}1 \cdot 0{,}090 = 0{,}339;$$
$$W_{B_4} = 0{,}520 \cdot 0{,}455 + 0{,}146 \cdot 0{,}455 + 0{,}3 \cdot 0{,}090 = 0{,}330.$$

Эти значения итоговых весов альтернатив позволяют остановиться на варианте B_3 как наиболее эффективном.

Методические указания к лабораторной работе

1. Сформировать бригады по три человека из студентов группы.
2. Назначить каждому члену бригады одну из ролей:

- технический директор – согласовывает финансирование проектов, связанных с технической модернизацией проекта в соответствующей области;
- системный администратор – обеспечивает компьютерное и программное обеспечения;
- разработчик информационных систем – отвечает за быстрый и надежный доступ к информации.

3. Для разработки вариантов интегрированной ИСОБТК провести анализ предметной области, указанной в варианте задания.
4. Используя МАИ, провести оценку предложенных проектов вариантов интегрированной ИСОБТК и выбрать оптимальный. Для этого:

а) назначить каждому члену бригады одну из ролей:

б) построить иерархическую модель поставленной задачи принятия решения;

в) задать матрицу сравнения, характеризующую степень относительного влияния каждого эксперта на окончательное решение;

г) каждому члену бригады в соответствии с выбранной ролью задать матрицу сравнения, характеризующую относительную важность используемых критериев;

д) для полученных матриц сравнения вычислить векторы соответствующих локальных приоритетов.

е) в соответствии с алгоритмом МАИ синтезировать вектор глобальных приоритетов и определить оптимальный вариант ИСОБТК.

5. Составить отчет к лабораторной работе с подробным изложением хода выполнения работы (включая иерархическую модель задачи принятия решений).

6. Сформулировать выводы и обосновать их.

Задания для самостоятельной работы

1. Выбрать вариант задания для самостоятельной работы.

2. Подготовить три предложения по проектированию интегрированной ИСОБТК в соответствии с одним из вариантов задания.

3. Оценить предложения методом анализа иерархий.

4. Подготовить отчет.

5. Представить результаты выполнения работы преподавателю.

Варианты задания

Разработать эскизный проект ИСОБТК для:

1) супермаркета;
2) участка цеха конвейерной сборки автомобильного завода;
3) малого предприятия розничной торговли;
4) городской клинической больницы;
5) железнодорожной станции;
6) мегаполиса;
7) промышленного региона.

Лабораторная работа №6

СИСТЕМЫ И СРЕДСТВА ПРОФЕССИОНАЛЬНОГО ОТБОРА ПРОИЗВОДСТВЕННОГО ПЕРСОНАЛА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Цель работы – обеспечить формирование у студентов навыков осуществления SWOT-анализа систем и средств профессионального отбора производственного персонала при обеспечении безопасности опасных производственных объектов (ОПО).

Теоретические сведения

Современные системы и средства профессионального отбора производственного персонала ОПО в интересах обеспечения безопасности промышленных объектов должны осуществлять поддержу принятия решений в отношении профпригодности оптанта на основе системного анализа комплекса психофизиологических, социально-психологических и социально-педагогических характеристик, а именно:

1) быстрота реакции;
2) точность выполнения рабочих операций;
3) устойчивость работы (к внешним воздействиям);
4) способность фокусировать внимание;
5) распределение внимания;
6) оперативно-динамическая память;
7) способность к формированию динамического образа ситуации;
8) способность к выделению главного в ситуации;
9) психологическая стрессоустойчивость;
10) способность к принятию ситуативных решений;
11) работоспособность центральная (умственная);
12) работоспособность периферическая (физическая);
13) способность к взятию ответственности за собственные решения;
14) интеллектуальная лабильность;
15) способность к прогнозированию развития ситуации;
16) склонность к риску;
17) возраст (от 20 до 45 – оптимум);
18) развитые образовательные компетенции;
19) опыт профессиональной деятельности (не менее 5 лет);
20) повышение квалификации;
21) перманентное самообразование.

Для оптимизации выбора наиболее эффективных систем и средств профессионального отбора производственного персонала целесообразно использовать метод **SWOT-анализа.** Такой анализ проводится с помощью вспомогательных таблиц (матриц) и основан на анализе сильных и слабых

сторон системы или средства, а также возможностей и угроз, исходящих из окружающей среды. Простейшая форма представления результатов SWOT-анализа приведена в табл. 31.

Таблица 31

Простейшая форма матрицы SWOT-анализа

Внешние стороны системы (объекта, процесса)	Внутренние аспекты системы (объекта, процесса)	
	возможности	угрозы
сильные стороны	«сильные стороны – возможности» (СИВ)	«сильные стороны – угрозы» (СИУ)
слабые стороны	«слабые стороны – возможности» (СЛВ)	«слабые стороны – угрозы» (СЛУ)

Также в процессе выполнения SWOT-анализа рекомендуется составлять профиль среды, т. е. таблицу, в которой должны быть отмечены факторы среды, оказывающие или могущие оказать существенное влияние на организацию. Для каждого фактора определяется его важность для отрасли, влияние на организацию, направление данного влияния и подсчитывается совокупная степень воздействия по каждому фактору и в целом. Вспомогательные матрицы для SWOT-анализа представлены в табл. 32–39.

Таблица 32

Матрица возможностей для SWOT-анализа

Вероятность использования возможностей	Влияние		
	сильное	умеренное	малое
Высокая	ВС	ВУ	ВМ
Средняя	СС	СУ	СМ
Низкая	НС	НУ	НМ

Таблица 33

Матрица угроз для SWOT-анализа

Вероятность использования возможностей	Влияние			
	разрушение	критическое состояние	тяжелое состояние	легкие ушибы
Высокая	ВР	ВК	ВТ	ВЛ
Средняя	СР	СК	СТ	СЛ
Низкая	НР	НК	НТ	НЛ

Таблица 34

Составление профиля среды для SWOT-анализа

Фактор среды	Важность для отрасли *A*	Влияние на организацию *B*	Направление влияния *C*	Степень важности *D=A·B·C*
1 2 3 …				

Этап 1 – идентификация сильных и слабых сторон, возможностей и угроз для социальной сети как социотехнической системы.

Этап 2 – формирование матрицы SWOT-анализа.

В табл. 35 представлена матрица SWOT-анализа.

Таблица 35

Матрица SWOT-анализа

Характеристики системы		Интенсивность (*Ai*)	Возможности (*O*)			Угрозы (*T*)		
			O_1	O_2	O_3	T_1	T_2	T_3
Вероятность появления (*Pj*)								
Коэффициент влияния (*Kj*)								
Сильные стороны (*S*)								
S_1								
S_2								
S_3								
Слабые стороны (*W*)								
W_1								
W_2								
W_3								

В строке *Pj* указывается вероятность появления конкретных возможностей и угроз. *Pj* может принимать значения в интервале от 0 до 1. При заполнении матрицы рекомендуется использовать шкалу, указанную в табл. 36.

Таблица 36

Шкала оценки вероятностей для SWOT-анализа

Качественная характеристика вероятности появления события	Числовое значение
Низкая вероятность	0,1–0,3
Средняя вероятность	0,4–0,6
Высокая вероятность	0,7–0,9
Очень высокая вероятность	1

В строке *Kj* указывается значение коэффициента влияния на деятельность ОПО конкретных возможностей и угроз, находящееся в пределах от 0 до 1 (табл. 37):

Таблица 37

Шкала оценки факторов влияния ОПО для SWOT-анализа

Значение	Интерпретация
0	Влияние отсутствует
1	Создаются совершенные новые возможности для деятельности организации или если реализация угрозы может повлечь прекращение деятельности
0,1–0,3	Влияние слабое
0,4–0,6	Влияние среднее
0,7–0,9	Влияние сильное

В столбце *Ai* проставляется значение интенсивность сильных и слабых сторон организации, при этом используется пятибалльная шкала. Шкала оценки для определения интенсивности сильных сторон представлена в табл. 38.

Оценка интенсивности слабых сторон выполняется аналогичным образом, но со знаком «минус».

Таблица 38

Шкала оценки интенсивности сильных сторон ОПО для SWOT-анализа

Балльная оценка	Интерпретация
5	Интенсивность высокая (очень сильное преимущество)
3–4	Интенсивность средняя (достаточно сильное преимущество)
1–2	Незначительное преимущество

В табл. 35 в ячейках O_1–O_3 и T_1–T_3 указываются способность сильных сторон содействовать реализации возможностей и противостоять угрозам и способность слабых сторон ослабить воздействие возможностей и усилить угрозы. Для упрощения процесса оценки рекомендуется использовать шкалу, представленную в табл. 39.

Таблица 39

Шкала оценки взаимосвязи сильных и слабых сторон с возможностями и угрозами

Балльная оценка	Интерпретация
5	Фактор дает полную возможность использовать благоприятные события или предотвратить отрицательные последствия угроз
4, 3	Существенное содействие использованию благоприятных возможностей или защите от угроз
1, 2	Незначительное влияние на использование благоприятных возможностей или защиту от угроз

Оценки в этих квадрантах должны выставляться без учета реальной интенсивности фактора для организации, т. к. это уже учтено в столбце интенсивность (*Aj*).

Этап 3 – преобразование матрицы.

Преобразование исходной матрицы осуществляется на основании следующей формулы:

$$Aij = Ai \cdot Kj \cdot Pj.$$

Затем производится суммирование полученных оценок по строкам и столбцам матрицы, а также разработка выводов и рекомендаций.

Пример SWOT-анализа для профессионального отбора персонала ОПО

Предположим, что экспертами предложен набор характеристик, представляющих сильные и слабые стороны, а также возможности их проявить и угрозы (риски) для осуществления успешной профессиональной деятельности, предъявляемые производственному персоналу ОПО:

Сильные стороны:

S_1 – способность к прогнозированию развития ситуации;

S_2 – перманентное образование и самообразование;

S_3 – высокая стрессоустойчивость.

Слабые стороны:

W_1 – нерациональное распределение внимания;

W_2 – сниженная устойчивость работы (к внешним воздействиям);

W_3 – возраст старше 45 лет.

***Возможности*:**

O_1 – повышение квалификации в процессе деятельности;

O_2 – реализация идей в рамках проектов;

O_3 – карьерный рост.

***Угрозы*:**

T_1 – профессиональная деятельность в условиях информационного стресса;

T_2 – склонность к риску;

T_3 – необходимый опыт профессиональной деятельности (не менее 5 лет).

	A	B	C	D	E	F	G	H	I	J	K	L
1												
2		Оценки	Возможности (О)					Угрозы (Т)				
3			O1	O2	O3			T1	T2	T3		
4	Сильные стороны (S)		1	1	1	3		5	5	5	15	
5	S1	10	10	10	10	30	90	50	50	50	150	450
6	S2	10	10	10	10	30		50	50	50	150	
7	S3	10	10	10	10	30		50	50	50	150	
8	Итого:	30	30	30	30			150	150	150		
9	Слабые стороны (W)											
10	W1	1	1	1	1	3	9	5	5	5	15	45
11	W2	1	1	1	1	3		5	5	5	15	
12	W3	1	1	1	1	3		5	5	5	15	
13	Итого:	3	3	3	3			15	15	15		
14												
15												

Рис. 12. Скриншот шаблона электронной таблицы в MS Excel 2010 для SWOT-анализа условий для профессионального отбора персонала ОПО

Примечание. Параметры для SWOT-анализа можно представлять по 3-, 5-, 10-, 100-балльным шкалам и более.

Для осуществления комплексного SWOT-анализа целесообразно использовать пять показателей, полученных в результате выполнения ряда междисциплинарных исследований:

– интегральный показатель SWOT-анализа:

$$K_{SWOT} = \frac{\left(\sum_{i=1}^{n} S_i + \sum_{i=1}^{n} W_i\right) \cdot \left(\sum_{i=1}^{n} O_i - \sum_{i=1}^{n} T_i\right)}{\sum_{i=1}^{n} O_i \cdot \sum_{i=1}^{n} T_i}; \quad (21)$$

– дискриминант *SOWT* («возможности и сильные стороны (*SO*) – угрозы и слабые стороны» (*WT*)):

$$D_{SOWT} = \sum_{i=1}^{n}\prod_{j=1}^{m} S_i O_j - \sum_{i=1}^{n}\prod_{j=1}^{m} W_i T_j ; \quad (22)$$

– дискриминант *WOST* («слабые стороны и возможности (*WO*) – сильные стороны и угрозы (*ST*))»:

$$D_{WOST} = \sum_{i=1}^{n}\prod_{j=1}^{m} W_i O_j - \sum_{i=1}^{n}\prod_{j=1}^{m} S_i T_j ; \quad (23)$$

– индекс «сильные стороны/слабые стороны»:

$$K_{S/W} = \frac{\sum_{i=1}^{n} S_i}{\sum_{i=1}^{n} W_i} ; \quad (24)$$

– индекс «возможности/угрозы»:

$$K_{O/T} = \frac{\sum_{i=1}^{n} O_i}{\sum_{i=1}^{n} T_i} . \quad (25)$$

Для оценки эффективности профессионального отбора оперативного персонала ОПО предложены показатели вероятности, основанные на величинах K_{SWOT}, $K_{S/W}$ и $K_{O/T}$ соответственно:

$$P_{SWOT} = \frac{K_{SWOT(\text{факт})}}{K_{SWOT(\max)}} ; \quad (26)$$

$$P_{S/W} = \frac{K_{S/W(\text{факт})}}{K_{S/W(\max)}} ; \quad (27)$$

$$P_{O/T} = \frac{K_{O/T(\text{факт})}}{K_{O/T(\max)}} . \quad (28)$$

Точность вероятностной оценки можно оценить с помощью показателя δ:

$$\delta = \sqrt{\left(P_{SWOT} - \langle P \rangle\right)^2 + \left(P_{S/W} - \langle P \rangle\right)^2 + \left(P_{O/T} - \langle P \rangle\right)^2} , \quad (29)$$

где $\langle P \rangle$ – среднее значение от суммы вероятности P_{SWOT}, $P_{S/W}$ и $P_{O/T}$.

Условие эффективности вероятностной оценки SWOT-анализа для профессионального отбора персонала ОПО:

$P_{SWOT} \to \max$; $P_{S/W} \to \max$; $P_{O/T} \to \max$; $\delta \to 0$.

На основе эмпирических исследований предложены нечеткие диапазоны значений показателей SWOT-анализа (табл. 40).

Таблица 40

Таблица диапазонов значений показателей SWOT-анализа

Показатели SWOT-анализа	Диапазоны значений показателей SWOT-анализа		
	<0	≈0	>0
K_{SWOT}	Преимущество угроз (рисков) над возможностями	Баланс возможностей над угрозами (рисками)	Преимущество возможностей над угрозами (рисками)
D_{SOWT}	Преимущество слабых сторон и угроз (рисков) над сильными сторонами и возможностями	Баланс взаимодей-ствия слабых сторон и угроз (рисков) и сильных сторон и возможностей	Преимущество сильных сторон и возможностей над слабыми сторонами и угрозами (рисками)
D_{WOST}	Преимущество сильных сторон и угроз (рисков) над слабыми сторонами и возможностями	Баланс между слабыми сторонами и угрозами (рисками) и сильными сторонами и угрозами (рисками)	Преимущество слабых сторон и возможностей над сильными сторонами и угрозами (рисками)
	<1	≈1	>1
$K_{S/W}$	Преимущество слабых сторон над сильными	Баланс сильных и слабых сторон	Преимущество сильных сторон над слабыми
$K_{O/T}$	Преимущество угроз (рисков) над возможностями	Баланс между возможностями и угрозами (рисками)	Преимущество возможностей над угрозами (рисками)

Задания для самостоятельной работы

Выполнить 3 варианта из нижеследующих заданий (табл. 41).

Таблица 41

Варианты заданий для SWOT-анализа профессионального отбора персонала ОПО на основе психофизиологических характеристик человека

Психофизиологические показатели	Варианты заданий									
	1	2	3	4	5	6	7	8	9	10
Быстрота реакции	+3	–1	+2	0	+1	–2	–1	+2	0	–3
Точность выполнения рабочих операций	+2	+3	0	–2	+1	–1	+2	0	+1	+2
Устойчивость работы (к внешним воздействиям)	0	+2	+1	+3	–3	+1	0	–2	+1	+3
Способность фокусировать внимание	+2	+1	–1	+3	2	–2	+2	0	+3	–1
Распределение внимания	0	+2	+1	–3	+3	–1	+2	–3	+1	–2

Окончание табл. 41

Психофизиологические показатели	Варианты заданий									
	1	2	3	4	5	6	7	8	9	10
Оперативно-динамическая память	–3	+1	–2	+3	+2	–2	+1	+3	+2	–3
Способность к формированию динамического образа ситуации	+3	0	–2	+2	–2	–1	0	-3	+3	+2
Способность к выделению главного в ситуации	–2	+2	У3	–3	0	–1	+2	+3	–2	–3
Психологическая стрессоустойчивость	–3	–2	0	+3	+1	0	+1	0	–3	+2
Способность к принятию ситуативных решений	0	+3	+3	–3	+3	В2	+2	–1	0	+3
Работоспособность центральная (умственная)	+2	–2	0	+3	–2	+2	+1	0	–2	+3
Работоспособность периферическая (физическая)	В3	+2	–2	+3	+3	–3	0	–1	+1	–2
Ответственность за собственные решения	–3	+2	0	+1	+2	0	+3	–2	0	–3
Интеллектуальная лабильность	0	+3	–2	0	–1	+3	0	–3	+2	–1
Способность к прогнозированию развития ситуации	–2	+3	+1	+3	0	У3	У2	0	–2	+1
Склонность к риску	–3	0	+3	–2	–2	–1	0	–2	–3	0
Возраст (от 20 до 45 – оптимум)	–2	0	+3	+2	+1	0	+1	+3	+3	–3
Развитые образовательные компетенции	–2	–3	+2	0	+3	+2	–2	–1	–2	+3
Опыт профессиональной деятельности (не менее 5 лет)	+3	–2	0	–3	+1	–2	+3	–1	0	+3
Повышение квалификации	–3	+3	–2	–3	0	–2	+3	+2	–2	0
Перманентное самообразование	–3	0	–2	+3	–2	0	–1	+3	–3	+2

Примечание. Здесь «+» – характеристика отнесена к сильным свойствам персонала в данных условиях деятельности; «–» – характеристика отнесена к слабым свойствам персонала в данных условиях деятельности; «У» – угроза; «В» – возможность. Каждая характеристика оценена по трехбалльной шкале.

Варианты заданий для самостоятельной работы

Варианты заданий для самостоятельной работы представлены в табл. 42.

Таблица 42

Варианты заданий и номера задач для лабораторной работы №6

Вариант	**Номера задач**	**Вариант**	**Номера задач**
1	1, 11	13	3, 8
2	2, 12	14	4, 7
3	3, 13	15	5, 6
4	4, 14	16	12, 19
5	5, 15	17	13, 18

Окончание табл. 42

Вариант	Номера задач	Вариант	Номера задач
6	6, 16	18	14, 17
7	7, 17	19	15, 16
8	8, 18	20	5, 16
9	9, 19	21	6, 17
10	10, 20	22	7, 18
11	11, 21	23	8, 19
12	2, 9	24	9, 20

Лабораторная работа №7

СИСТЕМЫ И СРЕДСТВА МОНИТОРИНГА ФУНКЦИОНАЛЬНОГО СОСТОЯНИЯ ПРОИЗВОДСТВЕННОГО ПЕРСОНАЛА

Цель работы – усвоение студентами теоретических и методологических основ использования простых, доступных и эффективных методов анализа функционального состояния оперативного персонала ОПО.

Теоретические сведения

Доля инцидентов со сложными промышленными системами и ОПО по причине ошибок человека достигает 75 % и более, нередко сопровождается авариями и катастрофами, связанными с человеческими жертвами, значительным экономическим и экологическим ущербом.

Метод критериального анализа надежности персонала производственных объектов

Анализ профессиональной деятельности оперативного персонала ОПО с позиций деятельностно-типологического подхода позволяет выделить сравнительно устойчивые классы типичных действий персонала ОПО в процессе профессиональной деятельности [6]:

1) правильно и своевременно выполненные действия, q_1 (усл. ед., %);
2) задержанные или невыполненные действия, q_2 (усл. ед., %);
3) неправильно выполненные действия, q_3 (усл. ед., %);
4) действия, выполненные с опозданием, q_4 (усл. ед., %);
5) действия, выполненные преждевременно, q_5 (усл. ед., %);
6) избыточные высказывания, шаги и действия при выполнении профессиональной деятельности, q_6 (усл. ед., %);
7) нерациональные действия, не способствующие успешному выполнению профессиональной деятельности, q_7 (усл. ед., %).

Для оценки и анализа безопасности и надежности профессиональной деятельности оперативного персонала наиболее целесообразно использовать следующие критерии:

1) эффективность решения профессиональных задач (ЭРПЗ) – условие высокой надежности профессиональной деятельности и безопасности функционирования ОПО в условиях информационного стресса при напряженной профессиональной деятельности:

$$\text{ЭРПЗ} = \frac{q_1}{\sum_{i=1}^{n} q_i}; \quad (30)$$

2) условие высокой надежности профессиональной деятельности и безопасности персонала ОПО в условиях информационного стресса при напряженной профессиональной деятельности: $\text{ЭРПЗ} \to 1$;

3) эффективность профессиональной деятельности:

$$\text{ЭПД} = 1 - \frac{q_2 + q_3 + q_4 + q_5 + q_6}{\sum_{i=1}^{n} q_i}; \quad (31)$$

4) уровень профессиональной подготовленности персонала (ППП):

$$\text{ППП} = \frac{q_3 + q_4}{\sum_{i=1}^{n} q_i}. \quad (32)$$

5) условие высокой профессиональной надежности и безопасности оперативного персонала ОПО, например, в условиях информационного стресса при напряженной профессиональной деятельности: $\text{ППП} \to 1$;

6) устойчивость результативности профессиональной деятельности (УРПД):

$$\text{УРПД} = 1 - \frac{q_5 + q_6}{\sum_{i=1}^{n} q_i}; \quad (33)$$

$$\text{УРПД} \to 1$$

7) активность переработки информации и принятия решений (АПИПР) при профессиональной деятельности:

$$\text{АПИПР} = 1 - \frac{q_4 + q_7}{\sum_{i=1}^{n} q_i}; \quad (34)$$

$$\text{АПИПР} \to 1.$$

Предложенные критерии зависят от специальности сотрудника ОПО, уровня и объема профессионального опыта, образования, индивидуально-типологических особенностей.

Деятельностно-типологическая методология анализа оператора производственного объекта

Охарактеризованы девять различных индивидуальных типов переработки информации и принятия решений операторами ОПО в ситуациях профессиональной деятельности: напряженный, неуверенный, заторможенный, агрессивно-анархический, детализирующий, дезорганизованный (суетливый), ложно-прогрессивный, временно-заторможенный, прогрессивный.

1. Напряженный тип. Процесс профессиональной деятельности проходит замедленно, напряженно, наблюдается общая заторможенность действий и процессов переработки интенсивного потока различной профессиональной информации и принятия решений в сложных ситуациях профессиональной деятельности. Внешние проявления: моторная заторможенность оператора, напряженная поза, чрезмерно напряженное сосредоточение при выполнении профессиональной деятельности. Для операторов – представителей данного типа переработки информации и принятия решений в профессиональной деятельности характерны повышенные значения критериев q_4 и q_7:

$$\frac{q_4 + q_7}{\sum_{i=1}^{n} q_i} \to 1. \qquad (35)$$

2. Неуверенный тип избегает сколько-нибудь решительных или рискованных действий, не склонен к значительным обобщениям и глобальным выводам, письменные ответы нечеткие, устные содержат много второстепенной информации; при выполнении тестов на профессиональную пригодность стремится оттянуть время, сверить ответ с другими отвечающими, прибегает к дополнительным консультациям. Для представителей этого типа характерна высокая сумма показателя задержанных или невыполненных действий (q_2), действий, выполненных с опозданием (q_4) и избыточных высказываний, шагов и действий при выполнении профессиональной деятельности (q_6):

$$\frac{q_2 + q_4 + q_6}{\sum_{i=1}^{n} q_i} \to 1. \qquad (36)$$

3. Заторможенный тип. В условиях лимита времени и/или при выполнении профессиональной деятельности в ситуациях повышенной сложности часто развивается общая заторможенность и прекращение деятельности. Для представителей этого типа характерен высокий показатель задержанных или невыполненных действий:

$$\frac{q_2}{\sum_{i=1}^{n} q_i} \to 1. \qquad (37)$$

4. Агрессивно-анархический тип характеризуется ослабленным самоконтролем либо его полной потерей, напористостью, агрессивностью на фоне отсутствия четкой общей цели действий. Для этого типа характерен высокий показатель неправильно выполненных и избыточных действий:

$$\frac{q_3 + q_6}{\sum_{i=1}^{n} q_i} \to 1. \qquad (38)$$

5. Детализирующий тип характеризуется уходом в мелочи, отсутствием представления об общей цели на фоне неплохого выделения общего направления; занимается второстепенными вопросами, не способствующими решению главной задачи. Для этого типа характерен высокий показатель нерациональных действий:

$$\frac{q_7}{\sum_{i=1}^{n} q_i} \to 1. \qquad (39)$$

6. Дезорганизованный (суетливый) тип хронически затрудняется принять верное решение либо выбрать одно из нескольких вариантов; непрерывно перебирает различные варианты решений задач профессиональной деятельности (теста, ситуации), мечется от одного решения к другому. Для этого типа характерен высокие показатели преждевременных и избыточных действий:

$$\frac{q_5 + q_6}{\sum_{i=1}^{n} q_i} \to 1. \qquad (40)$$

7. Ложно-прогрессивный тип действует активно и самоуверенно, достаточно быстро и напористо, чаще всего по неправильно выбранному пути и совершает много ошибок. Отсутствует склонность к рефлексии, самоанализу и самоконтролю. Для этого типа характерны высокие показатели неправильно выполненных и нерациональных действий:

$$\frac{q_3 + q_7}{\sum_{i=1}^{n} q_i} \to 1. \qquad (41)$$

8. Временно-замедленный тип характеризуется сложной организацией профессиональной деятельности: если в начале выполнения своих функциональных обязанностей присутствует заторможенность, то потом оператор активно включается в работу и обычно быстро и корректно справляется с заданием. Для представителей этого типа характерен высокий показатель критериев q_4, q_7, q_1:

$\frac{q_4 + q_7}{\sum_{i=1}^{n} q_i} \to 1$ – накануне социоинженерной атаки;

$\frac{q_1}{\sum_{i=1}^{n} q_i} \to 1$ – в процессе развития социоинженерной атаки.

9. Прогрессивный тип характеризуется способностью к высокой концентрации и мобилизации (волевой, эмоциональной, интеллектуальной), внутренних резервов в процессе выполнения сложных и продолжительных заданий. При напряженной работе и концентрации на проблеме находит оптимальное решение поставленной задачи. Показатель ЭРПД → 1.

Величина вышеуказанных показателей более чем на 0,6 свидетельствует о принадлежности данного оператора к конкретному типу профессиональной деятельности.

Пример анализа оператора ОПО на основе деятельностно-типологической характеристики

На основе экспериментальных и практических наблюдений за процессом профессиональной деятельности оперативного персонала ОПО были определены критерии безопасности и надежности профессиональной деятельности операторов систем управления ОПО (табл. 43) и дана их деятельностно-типологическая характеристика (табл. 44).

Таблица 43

Критерии безопасности и надежности профессиональной деятельности операторов систем управления ОПО (в усл. ед.)

Критерий безопасности и надежности профессиональной деятельности	Показатель класса действий						
	q_1	q_2	q_3	q_4	q_5	q_6	q_7
	85	10	5	5	5	10	5
ЭРПД = $\frac{q_1}{\sum_{i=1}^{n} q_i}$	0,68						
ЭПД = $1-\frac{q_1+q_3+q_4+q_5+q_6}{\sum_{i=1}^{n} q_i}$	0,12						
ППП = $\frac{q_3+q_4}{\sum_{i=1}^{n} q_i}$	0,08						
УРПД = $1-\frac{q_5+q_6}{\sum_{i=1}^{n} q_i}$	0,88						
АПИПР = $1-\frac{q_4+q_7}{\sum_{i=1}^{n} q_i}$	0,92						

Таблица 44

Деятельностно-типологическая характеристика операторов систем управления ОПО (в усл. ед.)

Критерий	Деятельностно-типологическая характеристика оператора	Показатель, усл. ед.
$\frac{q_4+q_7}{\sum_{i=1}^{n} q_i} \to 1$	Напряженный тип	0,08
$\frac{q_2+q_4+q_6}{\sum_{i=1}^{n} q_i} \to 1$	Неуверенный тип	0,16
$\frac{q_2}{\sum_{i=1}^{n} q_i} \to 1$	Заторможенный тип	0,08
$\frac{q_3+q_6}{\sum_{i=1}^{n} q_i} \to 1$	Агрессивно-анархический тип	0,08
$\frac{q_7}{\sum_{i=1}^{n} q_i} \to 1$	Детализирующий тип	0,04
$\frac{q_3+q_7}{\sum_{i=1}^{n} q_i} \to 1$	Дезорганизованный (суетливый) тип	0,08
$\frac{q_5+q_6}{\sum_{i=1}^{n} q_i} \to 1$	Ложно-прогрессивный тип	0,12
$\frac{q_4+q_7}{\sum_{i=1}^{n} q_i} \to 1$	Временно-замедленный тип	0,08
$\frac{q_1}{\sum_{i=1}^{n} q_i} \to 1$		0,68
$\frac{q_1}{\sum_{i=1}^{n} q_i} \to 1$	Прогрессивный тип	0,68

На основе анализа вышеуказанных коэффициентов возможна коррекция надежности и поведения операторов в условиях профессиональной деятельности для повышения ее эффективности.

Вывод. Очевидно, что оператор системы управления ОПО характеризуется высокими показателями ЭРПД, УРПД и АПИПР. Это свидетельствует о его профессиональной надежности.

Задания для самостоятельной работы

Варианты заданий для самостоятельной работы и используемые в них показатели действий представлены в табл. 45.

Таблица 45

Варианты заданий для лабораторной работы №7

Вариант задания	Показатель класса действий						
	q_1	q_2	q_3	q_4	q_5	q_6	q_7
1	8	16	25	35	55	73	7
2	65	13	15	35	10	30	15
3	65	77	25	3	13	30	15
4	85	20	4	15	25	15	10
5	78	10	15	25	52	22	14
5	89	5	12	10	52	35	17
6	90	20	8	12	25	18	44
7	95	13	4	15	9	12	11
8	80	11	3	20	2	11	22
9	75	9	17	27	15	18	9
10	65	7	8	8	10	19	3

Контрольные вопросы

1. Дайте определение понятию «риск».
2. Охарактеризуйте функциональную надежность оперативного персонала производственного объекта.
3. Опишите метод критериального анализа надежности персонала производственных объектов.
4. Сформулируйте представление о деятельностно-типологической методологии анализа оператора производственного объекта.
5. Представьте сравнительное описание различных типов операторов ОПО согласно деятельностно-типологической характеристике.

Лабораторная работа №8

ОЦЕНКА И ПРОГНОЗИРОВАНИЕ ПРОФЕССИОНАЛЬНОЙ НАДЕЖНОСТИ ПЕРСОНАЛА ОБЪЕКТОВ ОПАСНОГО ПРОИЗВОДСТВА

Цель работы – освоение студентами знаний и практических навыков анализа функциональной надежности персонала опасных производств.

Теоретические сведения

Функциональная надежность специалиста – это системное качество его организма, обеспечивающее возможность эффективной и успешной профессиональной деятельности. Функциональная надежность детерминирована комплексом физических, физиологических, психофизиологических и многих других характеристик.

Функциональная надежность персонала сложных технологических систем, включая опасные технологические производства, в значительной степени зависит от функционального состояния человека и динамики его индивидуальных психофизиологических характеристик (ПФХ).

В минимальном формате это состояние можно охарактеризовать на основе 13 ПФХ:1) быстрота реакции; 2) точность выполнения рабочих операций; 3) устойчивость работы (к внешним воздействиям); 4) способность фокусировать внимание; 5) распределение внимания; 6) оперативно-динамическая память (ОДП); 7) способность к формированию динамического образа ситуации; 8) способность к выделению главного в ситуации; 9) стрессоустойчивость; 10) способность к принятию ситуативных решений; 11) уровень утомляемости при умственной деятельности; 12) способность к взятию ответственности за собственные решения; 13) интеллектуальная лабильность.

Диапазоны функциональной надежности персонала

Эмпирически установлены четыре состояния функциональной надежности персонала ОПО при интенсивном информационном стрессе в процессе профессиональной деятельности. В связи с этим можно выделить четыре диапазона функциональной надежности персонала ОПО как вероятности: 1) низкая ($0<P<0,2$); 2) допустимая ($0,2\leq P<0,37$); 3) средняя ($0,37\leq P<0,63$); 4) высокая ($0,63\leq P<1,0$).

В табл. 46 представлены значения эталонных диапазонов психофизиологических характеристик, которые имеют важное значение для диагностики функциональной надежности персонала ОПО.

Таблица 46

Значения эталонных диапазонов психофизиологических характеристик, определяющих функциональную надежность персонала ОПО

Психофизиологическая характеристика	Методика	Измеряемый параметр	Единицы измерения	Значение a_{min}	Значение a_{max}
1. Быстрота реакции	Время реагирования на световой сигнал	Время реакции	мс	130	280
2. Точность выполнения рабочих операций	Реакция на движущийся объект	Доля точных реакций из всех реакций	%	8,8	15,6
	Воздействие на движущуюся стрелку при достижении ею неподвижной метки	Доля точных реакций из всех реакций	%	8	16
3. Устойчивость работы (к внешним воздействиям)	Простая сенсомоторная реакция на визуальные сигналы	Доля точных реакций из всех реакций	%	64	78
	Работоспособность при зрительно-моторной реакции	Время реакции	мс	140	510
4. Способность фокусировать внимание	Избирательность внимания	Доля правильных ответов из 150	%	83	94
	Концентрация и устойчивость внимания	Доля правильных ответов из 150	%	35	84
5. Распределение внимания	Переключаемость внимания	Время на переключение внимания	с	37,6	113,4
	Произвольность внимания	Время на выполнение задания	с	276	337
6. ОДП	Оценка оперативной памяти	Доля правильных ответов из 40	%	62	79
7. Способность к формированию динамического образа ситуации	Оценка степени устойчивости представлений	Уровень пространственных отклонений	мм	1,6	3,4
		Уровень временных отклонений	мс	150	480

Окончание табл. 46

Психофизиологическая характеристика	Методика	Измеряемый параметр	Единицы измерения	Значение a_{min}	Значение a_{max}
8. Способность к выделению главного в ситуации	Способность исключения избыточной информации	Доля правильных ответов из 40	%	69	86
	Идентификация зрительных стимулов	Доля правильных ответов из 40	%	73	92
9. Стрессоустойчивость	Степень психологической стрессоустойчивости	Уровень стрессоустойчивости	балл	0	100
10. Способность к принятию ситуативных решений	Прогностические способности	Доля правильных угадываний из 100	%	46	63
	Степень индивидуальности восприятия	Среднее время выполнения каждого из 30 заданий	с	4,5	13
11. Уровень умственной утомляемости	Способность к решению простых математических задач	Доля правильных ответов из 20	%	75	89
12. Способность к ответственности за собственные решения	Оценка стратегий принимаемых решений	Доля уравновешенных решений из 10	%	61	86
13. Интеллектуальная лабильность	Оценка способности переключения внимания на решение поступающих задач	Доля правильных ответов из 40	%	58	73

Методические рекомендации по выполнению работы

1. Внимательно изучите психофизиологические показатели функциональной надежности персонала, представленные в табл. 46, и данные «Методические рекомендации по выполнению работы».

2. Откройте на персональном компьютере электронную таблицу «НАДЕЖНОСТЬ_ПЕРСОНАЛА_ОПО (симуляция)» в MS Excel 2010 for Windows XP на странице «Психофизиологические показатели».

3. Приступите к выполнению задания в соответствии с данными, представленными в табл. 47.

4. После завершения заполнения электронной таблицы перейдите на страницу «Диаграмма» и изучите динамику функциональной надежности персонала ОПО при интенсивных эмоциональных и информационных нагрузках.

5. Выполните аппроксимацию (сглаживание) полученной диаграммы с помощью полиномиальной функции 6-й степени, зафиксируйте уравнение полученной функции аппроксимации и исследуйте ее на экстремумы.

6. На основе результатов исследования функции аппроксимации рассчитайте момент времени, когда функциональная надежность пользователя может достичь минимальных значений.

7. Сделайте выводы о характере динамики функциональной надежности персонала ОПО.

8. Ответьте на контрольные и дополнительные вопросы преподавателя.

9. Представьте преподавателю отчет о выполнении лабораторной работы в письменной форме.

Варианты заданий для самостоятельной работы

Таблица 47

Варианты заданий для самостоятельного выполнения в MS Excel 2010

Психофизиологические показатели	Вариант 1				Вариант 2				Вариант 3				Вариант 4			
	15	30	45	60	15	30	45	60	15	30	45	60	15	30	45	60
Быстрота реакции	5	10	15	25	10	20	30	40	10	25	50	50	10	30	50	70
Точность выполнения рабочих операций	10	10	20	30	5	10	15	20	10	10	20	20	10	20	30	50
Устойчивость работы (к внешним воздействиям)	5	5	10	10	5	10	15	20	5	10	20	30	10	30	45	60
Способность фокусировать внимание	5	10	15	20	10	20	30	40	5	5	10	15	10	15	20	30
Распределение внимания	5	10	20	30	5	5	10	20	10	20	30	40	5	5	10	20
Оперативно-динамическая память	10	20	30	40	5	10	15	20	5	15	30	50	5	10	10	20
Способность к формированию динамического образа ситуации	5	5	5	5	10	10	10	20	5	10	20	30	10	20	30	50
Способность к выделению главного	5	5	10	10	5	10	15	20	5	10	15	20	10	20	30	40
Психологическая стрессоустойчивость	5	5	5	15	5	10	15	20	5	10	20	30	10	20	30	40
Способность к принятию ситуативных решений	5	5	5	10	5	10	15	20	5	10	20	30	10	20	30	40
Уровень умственной утомляемости	5	5	10	15	5	10	20	30	10	15	25	35	10	20	30	50
Способность к принятию ответственности за решения	5	5	5	10	5	10	15	20	10	20	30	40	10	20	30	40
Интеллектуальная лабильность	5	5	10	15	5	10	15	20	10	10	30	40	5	15	30	50

Контрольные вопросы

1. Охарактеризуйте важнейшие факторы, оказывающие влияние на функциональную надежность персонала системы управления ОПО.

2. Перечислите психофизиологические характеристики, имеющие важнейшее значение для функциональной надежности персонала ОПО.

3. Охарактеризуйте диапазоны снижения функциональной надежности персонала ОПО.

ЛИТЕРАТУРА

1. Астахов, А. М. Искусство управления информационными рисками / А. М. Астахов. – М. : ДМК Пресс, 2010. – 312 с.
2. Барабанова, М. И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: учеб. пособие / М. И. Барабанова, В. И. Кияев. – СПб. : Изд-во СПбГУЭФ, 2013. – 267 с.
3. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – М. : Телеком, 2010. – 272 с.
4. Иванов, И. В. Охрана периметров / И. В. Иванов. – М. : Радио и связь, 1997. – 96 с.
5. Лагутин, В. С. Утечка и защита информации в телефонных каналах / В. С. Лагутин, А. В. Петраков. – М. : Энергоатомиздат, 1996. – 306 с.
6. Меркурьев, Г. В. Оперативно-диспетчерское управление энергосистемами: метод. пособие / Г. В. Меркурьев. – СПб., 2002. – 117 с.
7. Поздняков, Е. Н. Защита объектов (Рекомендации для руководителей и сотрудников служб безопасности) / Е. Н. Поздняков. – М. : Банковский деловой центр, 1997. – 224 с.
8. Попов, В. Г. Информационная техника и технологии, применяемые в УИС России / В. Г. Попов. – Томск : ООО «ДиВО», 2007. – 174 с.
9. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. – М. : Щит-М, 1999. – 254 с.
10. Рыжова, В. А. Проектирование и исследование комплексных систем безопасности / В. А. Рыжова. – СПб. : НИУ ИТМО, 2013. – 156 с.
11. Синилов, В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации : учебник / В. Г. Синилов. – М. : Академия, 2010. – 512 с.
12. Тихонов, И. А. Информативные параметры биометрической аутентификации пользователей информационных систем по инфракрасному изображению сосудистого русла / И. А. Тихонов // Биомедицинская техника и радиоэлектроника. – 2012. – №9. – С. 26–32.
13. Цирлов, В. Л. Основы информационной безопасности автоматизированных систем: краткий курс / В. Л. Цирлов. – Феникс, 2012. – 173 с.
14. «Шпионские штучки» и устройства для защиты объектов и информации: справ. пособие. – СПб. : Лань, 1996. – 266 с.
15. Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2004. – 384 с.
16. Ярочкин, В. И. Система безопасности фирмы / В. И. Ярочкин. – М. : Ось-89, 1997. – 192 с.

Св. план 2015, поз. 16

Учебное издание

Давыдовский Анатолий Григорьевич
Пилиневич Леонид Петрович
Савченко Владимир Владимирович и др.

СПЕЦИАЛИЗИРОВАННЫЕ СИСТЕМЫ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

ПОСОБИЕ

Редактор *М. А. Зайцева*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 27.04.2016. Формат 60х84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 4,07. Уч.-изд. л. 4,3. Тираж 50 экз. Заказ 204.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6