# Управление рисками и безопасностью

## Человеческий фактор как угроза транспортной безопасности

Г. Л. Смолян, Г. Н. Солнцева

**Аннотация**. Человеческий фактор определен как совокупность характеристик человеческих отношений и человеческого поведения, приводящая к нарушению безопасности объекта транспортной инфраструктуры или средства транспорта. Люди рассматриваются как источник противоправных террористических, криминальных и кибернетических угроз, как. источник опасных воздействий на организационные и управленческие структуры, программно-технические средства, административный, оперативный и обслуживающий персонал. В статье анализируются три основных класса опасных действий людей: умышленные действия, непреднамеренные ошибки персонала, нарушения требований к нормативной деятельности. Обсуждается подход к оценке рисков осуществления опасных действий персонала, основанный на регулярном проведении аудита (инспекционных проверок) всех случаев нарушения нормального функционирования объекта. Риски опасных действий связываются с рисками невыполнения требований по обеспечению безопасности и с соответствием отчетной информации реальному состоянию защищенности объекта. Полученные в результате инспекционных проверок данные служат основанием для определения количественных оценок степени доверия к надежности (качеству) выполнения персоналом объекта своих функций. Приводится стандартная таблица оценки степени доверия к персоналу.

**Ключевые слова:** *человеческий фактор, транспортная безопасность, угроза, опасные действия людей, персонал, оценка рисков, степень доверия.*

*Любая система, зависящая от человеческой надежности, ненадежна.*

Закон Мерфи

### Введение

Регулярные исследования роли человеческого фактора (ЧФ) в возникновении аварий и катастроф, в нарушении или снижении эффективности функционирования критических инфраструктур и объектов, основу которых составляют человеко-машинные системы (ЧМС), ведутся с 60-х годов прошлого века. Учет ЧФ на первых этапах сводился к изучению возможностей человека как звена ЧМС, к измерению его антропометрических и психофизиологических характеристик, к контролю и коррекции его функционального состояния, к грамотной организации подготовки и психологического отбора специалистов. Существенные результаты этого учета были достигнуты, прежде всего, в образцах вооружения и военной техники, создание которых собственно и стимулировало исследования ЧФ, в пилотируемой космонавтике, авиации, АЭС.

Тем не менее, на объектах транспортной инфраструктуры и средствах транспорта аварии и катастрофы несчастные случаи по вине человека происхо-

дят с ужасающей частотой. Примеры у всех на слуху: самолеты, паромы, «Фобос-грунт», столкновения поездов и автомобилей. По далеко неполной статистике действия людей приводят к авариям и катастрофам на автотранспорте в 57% случаев, на ж/д транспорте около 50%, в авиации и водном транспорте до 70% случаев [1]. Близкие цифры приводятся и в других источниках, например, в Государственном докладе МЧС за 2001–2002 годы.

А. Н. Либерман в монографии, посвященной в основном безопасности АЭС [2], убедительно показывает, что существует вполне реальная опасность увеличения частоты человеческих ошибок, вызванных различными причинами, на всех этапах создания и эксплуатации новой техники и технологий просто в силу отставания возможностей человека от развития (усложнения) техники. В мировой и отечественной литературе обычно разделяют два класса этих причин: внешние (организационные) и внутренние (индивидуально-личностные) причины отказов человека как компонента эргатической системы. Исходя из этого, можно дать следующее определение:

*Человеческий фактор — это совокупность характеристик человеческих отношений (организационная составляющая) и человеческого поведения (индивидуально-личностная составляющая), приводящая к прекращению или нарушению функционирования объекта.*

Это определение вполне согласуется с изложенным в [3] тезисом, что обеспечение безопасности КВО есть «создание условий, при которых действие внешних и внутренних факторов не приводит к ухудшению параметров состояния КВО или к невозможности его функционирования и развития».

## 1. Угрозы безопасности со стороны ЧФ

В литературе по безопасности критически важных объектов (КВО) наряду с постоянными природными и техногенными угрозами рассматривают террористические, криминальные и кибернетические угрозы [3]. Они и есть собственно угрозы незаконного вмешательства — противоправного действия (бездействия) людей Именно люди являются источником этих угроз, т. е. источником опасных воздействий на организационные и управленческие структуры, программно-технические средства, административный, оперативный и обслуживающий персоналы КВО, в том числе персонал системы обеспечения его безопасности, причем они могут находиться как вне КВО, так и внутри него. Противоправные, прежде всего террористические действия влекут за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создают угрозу наступления таких последствий;

Как свидетельствует практика последних десятилетий, угрозы противоправных акций сохраняются (а немало их было реализовано) для многих типовых объектов транспортной инфраструктуры:

– аэродромов, аэропортов, объектов систем навигации и управления движением транспортных средств;
– ж/д и автомобильных вокзалов и станций, тоннелей, мостов, морских терминалов, речных портов).

То же можно сказать и о средствах транспорта (самолетах, ж/д и метропоездах и др.). Перечень КВО транспортного комплекса приведен в Федеральном законе о транспортной безопасности [4].

Поскольку эти объекты насыщены автоматизированными информационно-вычислительными комплексами и системами (системы сигнализации и связи, различные классы АСУ, логистические центры, автоматизированные системы обеспечения безопасности и др.), серьезную опасность для них представляют и кибернетические угрозы.

Как справедливо указывает П. И. Серебрянников [5], «большинство аварий на всех видах транспорта происходит вследствие действий людей — или, во всяком случае, одной из причин аварий по итогам расследования обязательно называют именно их. Так, в судовождении это причина 70–80% всех крушений; аналогичные цифры указываются для авиации. В статистике железнодорожных катастроф чаще называется цифра 50%, но тут в «человеческом факторе» учитывают также ошибки и нарушения регламента при техническом обслуживании подвижного состава и путевого хозяйства. В автомобильном транспорте отдельной статистики аварий, происшедших по другим причинам, кроме ошибок водителя и нарушений правил, даже не ведется».

Это во многом дает основания для суждения о том, что человек является слабым звеном современных транспортных систем, и доводом в пользу увеличения доли автоматики в управлении движением. Это не совсем так, возражает этот автор: в расчете на пассажиро-километр высокоавтоматизированная железная дорога дает большее количество человеческих жертв, чем авиация и автобусные перевозки; это справедливо как для развитых стран (http://europa.eu.int/comm/transport/infr-charging/library/crash-cost.pdf), так и для России (http://www.css-mps.ru/zdm/05-1999/9031.htm).

Человеческий фактор нередко существенно дополняет другие причины аварий. Если самолет теряет управление и на крейсерской скорости врезается в землю, чаще все-таки имеет место сочетание факторов, скажем, посадка в незнакомом аэропорту в условиях плохой видимости или неисправность

техники, к которой ошибка экипажа *только добавилась.*

Есть три фундаментальных условия, порождающих угрозы безопасности КВО со стороны людей, т. е. три основных мотива нарушений:

– непрофессионализм, некомпетентность,
– самоутверждение,
– корыстный интерес или идеологическая установка (например, исламский джихад).

Независимо от того, где находится источник опасности, действия людей могут быть разделены на три основных класса:

А. Умышленные противоправные действия.
Б. Непреднамеренные ошибки персонала.
В. Нарушения требований к нормативной деятельности.

Ниже подробно рассматриваются эти классы угроз.

## 2. Умышленные противоправные действия

2.1. Теракты и другие насильственные действия. Транспортная инфраструктура, особенно дальних видов транспорта, представляет собой весьма привлекательную цель как для террористов, ибо она собирает в ограниченном пространстве много людей, так и для преступников, ибо многие из этих людей имеют при себе значительные ценности.

Вот примеры главных из этих действий:

1. Захват заложников с целью получения выкупа или выдвижения политических требований обязательно через освещение в СМИ.
2. Уничтожение пассажиров и грузов на борту транспортного средства, а также уничтожение иных объектов с использованием транспортного средства как инструмента.
3. Кражи и ограбления (от карманных краж в автобусах до морского пиратства включительно).

Хорошо известно, что смысл террора — в устрашении большого количества людей. Это то самое чувство, которое в первую очередь вызывается у людей террористическим актом. Психологи определяют страх как негативную эмоцию особой интенсивности, вызываемую надвигающимся бедствием. Первичными и наиболее глубинными причинами, вызывающими страх, являются боязнь физического повреждения и опасения смерти.

Страх редко ощущается при непосредственном приближении опасности. Как правило, страх овладевает человеком спустя некоторое время после опасной ситуации и продолжает преследовать его потом в аналогичных или похожих ситуациях. Так действует механизм «отложенного страха», на котором, в основном, и играют террористы [5].

Между террористическими и криминальными актами есть важное отличие, подчеркивается в [5]: в соответствии с законодательством Российской Федерации и ряда других стран, государство несет определенную материальную ответственность перед пострадавшими от терактов; отчасти это логически следует из определения терроризма, принятого в УК РФ:

*Терроризм — насилие или угроза его применения в отношении физических лиц или организаций, а также уничтожение (повреждение) или угроза уничтожения (повреждения) имущества и других материальных объектов, создающие опасность гибели людей, причинения значительного имущественного ущерба, осуществляемые в целях нарушения общественной безопасности, устрашения населения, или оказания воздействия на принятие органами власти решений, выгодных террористам, или удовлетворения их неправомерных имущественных и (или) иных интересов.*

Тем самым признаётся, что терроризм — это действия, направленные в первую очередь против органов власти и государства, и, соответственно, в большей мере проблема государства, чем граждан — даже если граждане и страдают от него.

Жертва обычного ограбления может рассчитывать на возврат своего имущества, только если правоохранительным органам удастся найти украденное. Поскольку это происходит довольно редко, граждане оказываются вынуждены дополнять государственную защиту от преступников собственными мерами, в том числе и страхованием.

Напротив, поскольку компенсации пострадавшим от терактов берет на себя государство, страховые компании часто отказываются считать теракты страховыми случаями. Это может оговариваться как явным образом при заключении страхового договора, так и задним числом (например, после терактов 11 сентября 2001 года).

Следует отметить, что СМИ в основном уделяют внимание терактам, в то время как собственно криминальная деятельность вызывает гораздо меньший интерес. Захваты заложников охотно и подробно освещаются СМИ, в то время как вооруженные ограбления автобусов с челноками или перегоняемых автомобилей настолько в порядке вещей, что освещаются только изредка в местной прессе.

2.2. Действия нелояльного персонала. К умышленным, противоправным действиям, помимо террористических и криминальных актов; следует отнести действия нелояльных сотрудников (обиженные сотрудники, работающие и бывшие, обозленные неудачники, инсайдеры и др.).

Как показывает мировой опыт, нелояльный персонал — неисчерпаемая база для формирования злоумышленников. Именно поэтому обеспечение лояльности персонала превращается из проблемы менеджмента и кадровых служб в проблему обеспечения безопасности. В общем случае лояльность в современных словарях определяется как установка на поведение, заключающаяся в соблюдении существующих правил, норм, предписаний, а также в выполнении своих обязанностей по отношению к другим даже при несогласии с ними. Лояльность персонала в организации часто понимается как психологическая связь между работником и организацией, базирующаяся на осознании работником своих обязательств по отношению к организации и снижающая вероятность того, что он добровольно оставит организацию или принесет ей вред [7].

Различают несколько типов поведения нелояльных сотрудников, которые представляют угрозу безопасности организации [8]:

*Аддиктивное поведение.* Уход от реальности вследствие изменения своего психического состояния, с помощью наркотиков, алкоголя или постоянной фиксации внимания на определенных предметах или видах деятельности (азартные игры), для получения интенсивных эмоций. Для этого человек может пожертвовать чем угодно.

Эти процессы управляют жизнью человека, делают его беспомощным, лишают воли.

*Антисоциальное поведение*. Основная черта — совершение действий, противоречащих принятым в обществе этическим принципам и нормам, безответственность, игнорирование прав других людей.

*Конформистское поведение*. Исполнение воли «авторитета», приспособленчество, некритичность, неспособность принимать решения, брать на себя ответственность.

*Фанатическое поведение*. Слепая приверженность какой-либо идее, нетерпимости к другим взглядам, что может сопровождаться действиями насильственного характера. Нейтральные или дружеские поступки других людей часто оцениваются как враждебные или заслуживающие презрения.

*Аутистическое поведение.* Затруднение социальных контактов, оторванность от действительности, погруженность в себя.

К категории нелояльных сотрудников следует отнести «обиженных» сотрудников, неудовлетворенных своим положением в организации — работающих и бывших. Как правило, их действиями руководит желание нанести вред организации — обидчику. Например, повредить оборудование; встроить логическую бомбу, которая со временем разрушит программу и/или данные; ввести неверные или изменить существующие данные и т. д. «Обиженные сотрудники» знакомы с порядками в организации и способны вредить очень эффективно. Чаще всего их действия существенно облегчаются тем, что система пересмотра и уточнения прав пользователей на доступ к информации крайне неповоротлива или отсутствует вовсе.

С. Горностаев [9] выделяет и ранжирует следующие нематериальные факторы, повышающие недовольство трудовой деятельностью в организации и влияющие на увеличение нелояльности как готовности сменить место работы, а в определенных случаях «отомстить»:

1) отсутствие справедливой оценки и признания результатов деятельности со стороны руководства как фактор оставления места работы отметили 65,8 % опрошенных;
2) невнимание или формальное отношение со стороны руководства организации и подразделения к личным и профессиональным проблемам сотрудника — 60 %;
3) отсутствие уважения к личности сотрудника со стороны руководства — 51,5 %;
4) низкая востребованность результатов труда и достижений по работе — 34,2 %;
5) невозможность самореализации на занимаемой профессиональной позиции и отсутствие перспектив карьеры в организации — 31,5 %;
6) отсутствие положительных эмоциональных связей и взаимопомощи между сотрудниками — 28,6 %;
7) конфликты в коллективе, отсутствие взаимопонимания с коллегами — 22,9 %;
8) отрицательное отношение к профессиональной деятельности в коллективе — 17,2 %;
9) авторитаризм руководства, управление без учета мнения сотрудников — 14,3 %;
10) содержание деятельности, не вызывающее интереса — 14,3 %.

2.3. Кибернетические угрозы, вызванные действиями людей (злоумышленников). На основе обобщения зарубежного опыта и состояния информационной безопасности в АФК «Система» Е. Г. Новицкий [10] приводит следующий перечень кибернетических угроз:

– Физическое разрушение системы или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы.
– Вывод из строя подсистем обеспечения функционирования информационно-вычислительных систем, в том числе системы обеспечения безопасности.
– Применение подслушивающих устройств, дистанционные фото- и видеосъемки и т. п.
– Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непо-

средственно не участвующие в обработке информации.
- Перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.
- Хищение носителей информации.
- Несанкционированное копирование носителей информации.
- Хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.).
- Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.
- Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме.
- Незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя.
- Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики (номер рабочей станции в сети, физический адрес, адрес в системе связи, и т. п.).
- Вскрытие шифров криптозащиты информации.
- Внедрение программных «закладок» и «вирусов» с целью регистрации и передачи критической информации или дезорганизации функционирования системы.
- Незаконное подключение к линиям связи с целью с использования пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений.
- Незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.
- Компрометация ключей шифрования.

Необходимо отметить, что чаще всего для достижения поставленной цели злоумышленник использует не одну угрозу, а некоторую комбинацию из перечисленных выше.

Особый вид умышленных действий составляют компьютерные преступления (компьютерное мошенничество, подделка компьютерной информации, повреждение данных или программ, компьютерный саботаж, несанкционированное вторжение в систему (доступ, перехват данных, использование незащищенных компьютерных программ), а также различные виды атак на системы управления базами данных, на операционные системы и сетевое программное обеспечение).

Для компьютерных преступлений последнего времени (для хакеров нового поколения) наиболее характерен интерес к новинкам компьютерной техники, устройствам связи и программным средствам [11].

Наиболее распространенными становятся атаки:
- на системы управления базами данных,
- на операционные системы,
- на сетевое программное обеспечение.

Для них типичны системная подготовка взлома, широкое использование агентурных и оперативно-технических методов, предварительная апробация системы методов взлома и предельно быстрое осуществление атаки, исключающее возможность зафиксировать факт ее осуществления и принятие контрмер по отражению, выявлению личности и местонахождения атакующего. Они точно рассчитывают рациональность методов взлома защиты компьютерной системы, разрабатывают программы действий, обеспечивающих анонимность атаки, никогда не действуя под собственным именем и тщательно скрывая свой сетевой адрес.

Новый XXI век стал веком мощных хакерских атак. Полностью их отразить еще не смогла ни одна система до сих пор. Одной из самых мощных атак, направленных на отказ в обслуживании, подверглись интернет-сайты eBay, Yahoo и Amazon.

Хакеры взломали внутрикорпоративную сеть Microsoft и получили доступ к исходным кодам последних версий Windows и Office. Корпорация Microsoft оказалась в числе самых крупных жертв хакеров, наносящих удары по серверам доменных имен (DNS). В результате атак, направленных на отказ в обслуживании, информация о маршрутах DNS, к которой обращались клиенты интернет-сайтов Microsoft, была уничтожена. Взлом обнаружили через несколько часов, но целых два дня миллионы пользователей не могли попасть на страницы Microsoft.

Мощные вирусные атаки перегружали компьютерные сети континентов и стран. В Южной Корее, после компьютерной вирусной эпидемии, в течение 2–3 дней не работали банкоматы, аэропорты, сеть Интернет и многое другое. Ущерб составил несколько миллиардов долларов. Конец 90-х годов XX в. и начало XXI в. — это этап институализации хакеров: создание крупных объединений, союзов, фирм, тесным образом сотрудничающих с криминальными и теневыми структурами, активная пропаганда ценностей и принципов хакерской субкультуры через средства массовой информации.

## 3. Непреднамеренные ошибки персонала

Самыми частыми и не менее опасными, чем действия злоумышленников (с точки зрения размера ущерба), являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационно-вычислительные системы КВО [12]. Иногда такие ошибки являются прямыми угрозами (неправильно введенные данные или команды), иногда они выступают как угрозы косвенные, создающие дополнительные уязвимости, которыми могут воспользоваться злоумышленники. Считается, что почти 65% потерь связано с непреднамеренными ошибками [13].

Приведем примерный перечень угроз, обусловленных непреднамеренными действиями людей относительно информационно-вычислительных ресурсов и средств системы, в том числе и систем обеспечения безопасности.

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.
2. Неправомерное включение оборудования или изменение режимов работы устройств и программ.
3. Неумышленная порча носителей информации.
4. Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществить необратимые изменения в ней.
5. Нелегальное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).
6. Заражение компьютеров вирусами.
7. Неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной.
8. Разглашение, передача или утрата атрибутов разграничения доступа.
9. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации.
10. Игнорирование организационных ограничений и административных регламентов.
11. Вход в систему в обход средств защиты.
12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности.
13. Пересылка данных по ошибочному адресу абонента (устройства).
14. Ввод ошибочных данных.
15. Неумышленное повреждение каналов связи.

Как уже отмечалось выше, есть три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо деструктивные действия. В большинстве случаев это следствие некомпетентности или небрежности.

Профессиональная деятельность персонала в любых системах регламентирована нормами и правилами выполнения функциональных задач. Любые нарушения, отклонения от нормативной выступают как угрозы безопасности и могут приводить к непоправимым последствиям. Возможность нарушений делает профессиональную деятельность персонала одним из самых уязвимых звеньев в человеко-машинных системах обработки и передачи информации.

Рассмотрим подробнее природу ошибок.

Под ошибкой человека в системе понимается результат действия, не соответствующий требуемому параметру нормативной деятельности, т. е. ошибки определяются только в отношении предписанных действий, в силу чего вероятность ошибок является одним из показателей качества деятельности. При анализе ошибок они разделяются по частоте и степени влияния на результат.

Результат неумышленных ошибочных действий, как правило, осознается только после их совершения. Они носят либо случайный, либо систематический характер. Минимизация случайных ошибок, их предупреждение обычно достигается специальными программными средствами контроля и исправления ошибок. Причиной систематических ошибок в общем случае является несоответствие возможностей и ограничений человека в выполнении профессиональных функций в системе, параметрам и условиям функционирования программно-технических средств. В настоящее время имеется более или менее достаточные справочные данные о параметрах деятельности человека и их динамике[14]. Их и следует учитывать для уменьшения вероятности ошибочных действий. Это такие характеристики как, например, скорость обработки информации различного типа при различных режимах ее предъявления, скорость и точность движений, помехоустойчивость и др. при решении различных задач.

Систематические ошибки появляются также вследствие несоответствия жестко фиксированных параметров функционирования программно-технических средств вариабельности параметров деятельности. Вариабельность связана с динамикой психиче-

ских процессов и других составляющих деятельности как у разных профессионалов (разброс индивидуально-личностных особенностей), так и у отдельного человека в процессе деятельности. Основными факторами, определяющими динамику параметров человека, являются выраженность профессионально-важных качеств, в том числе готовность и устойчивость, уровень профессиональной подготовки и компетентности, текущее функциональное состояние.

Анализ содержания ошибок показывает, что в качестве элементарных ошибок в действиях человека выступают:

- при приеме и передаче информации — пропуск символа или слова, ошибочные опознания, идентификация или классификация данных, неадекватная реакция на сообщение, задержка в передаче данных, неправильное декодирование, неправомерная ассоциация с другими сообщениями и т. п.;
- при принятии решения — забывание или искажение информации, неправильная оценка возможных последствий, учет ограниченного числа сообщений и т. п.

Типичные следствия таких ошибок:

- искажение или потеря информации;
- вывод из строя или разрушение носителей информации;
- вывод из строя или разрушение программных или технических средств;
- нарушение технологии, алгоритмов или процедур выполнения функциональных задач.

Уменьшение вероятности таких ошибок представляется важной задачей, решение которой следует искать на путях постоянного контроля уровня подготовки и функционального состояния. В литературе приводятся вероятностные характеристики подобного рода ошибок при выполнении сложных и простых (отдельные операции) действий [15]. Они определяются, как правило, экспериментальным путем на основании большого количества замеров. Эти данные показывают, что вероятность безошибочной работы во многом зависит от уровня эргономического обеспечения проектировочных решений, и может составлять, например, для поиска, восприятия и декодирования информации — от 0,95 до 0,995; для принятия решения — от 0,9 до 0,995; выполнения принятого решения — от 0,92 до 0,995 в зависимости от сложности работы с техническими средствами.

Следует отметить, что все имеющиеся способы расчета и данные об эмпирических зависимостях безошибочности деятельности от отдельных факторов охватывают преимущественно частные случаи и без специальных дополнительных исследований не могут быть непосредственно использованы для обеспечения безопасности деятельности персонала на критически важных объектах. Это означает, что необходимо проводить постоянный мониторинг ошибок оперативного и обслуживающего персонала и его результаты учитывать при организации подготовки (переподготовки) и тренировки персонала. Немаловажную роль в предупреждении непреднамеренных ошибок могут сыграть и специально встраиваемые в аппаратуру средства контроля и исправления ошибок. Опыт использования подобных средств имеется во многих автоматизированных системах ответственного назначения (в оборудовании АЭС, обитаемых космических кораблей и др.).

Меры предотвращения угроз безопасности, связанных с непреднамеренными ошибками, должны предусматривать соблюдение эргономических требований в части допустимой информационной нагрузки, обеспечения комфортных условий работы и дружественности пользовательского интерфейса, требований к режиму труда и отдыха.

Для персонала КВО необходимо проводить отбор работников по выделенным профессионально-важным качествам в такой же степени, в какой производится отбор оперативного персонала для автоматизированных систем специального назначения.

Повторим еще раз : люди являются необходимым звеном системы. С другой стороны — они же являются основной причиной и движущей силой нарушений и преступлений. В этом смысле вопросы безопасности информационно-вычислительных систем суть по большому счету вопросы человеческих отношений и человеческого поведения.

По отношению к системам КВО нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала:

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники),
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС);
- сотрудники службы безопасности ИС;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности объекта (энерго-, водо-, теплоснабжения и т. п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность ИС);
- любые лица за пределами контролируемой территории.

Мировой и отечественный опыт эргономического обеспечения деятельности людей в человеко-машинных (эргатических) системах показывает, что имеется немало средств предотвращения или минимизации угроз, связанных с непреднамеренными ошибками людей. Они могут быть систематизированы следующим образом.

1. Организация внешних средств деятельности персонала:
   1.1. Определение информационной нагрузки (соблюдение требований к объему, сложности, скорости, форме подачи информации).
   1.2. Выбор и организация аппаратно-технических средств (соблюдение требований к удобству работы человека с комплексом технических средств).
   1.3. Организация взаимодействия человека с программными средствами (обеспечение дружественности пользовательского интерфейса).
   1.4. Организация рабочей среды персонала (соблюдение требований к характеристикам окружающей среды на рабочем месте, к режиму труда и отдыха).
2. Организация внутренних средств деятельности персонала.
   2.1. Организация профессионального отбора по выделенным профессионально-важным качествам (отбор по показателям свойств нервной системы, темперамента, эмоциональной устойчивости).
   2.2. Организация обучения персонала (методическое обеспечение передачи необходимых знаний, тренировки навыков и умений, поведения в различных ситуациях).
3. Поддержка психологической структуры деятельности.
   3.1. Диагностика, формирование и отбор по заданным критериям целей, мотивов, ценностей, направленности, черт личности.
   3.2. Совершенствование организационной структуры в целях создания оптимального социально-психологического климата (перераспределение функций и обязанностей, формирование рабочих групп).

## 4. Оценка рисков осуществления опасных действий персонала КВО

Важным инструментом оценки риска опасных действий персонала КВО, приводящих к полному или частичному прекращению функционирования объекта, является регулярное проведение аудита (инспекционных проверок) всех случаев нарушения нормального функционирования КВО. В результате должна определяться эффективность действий персонала по различным сценариям развития опасных ситуаций.

В практическом плане она связывает риски опасных действий с рисками невыполнения требований по обеспечению безопасности и с соответствием отчетной информации реальному состоянию защищенности объекта [3]. Эти случаи должны охватывать все действия, рассмотренные выше. При этом следует понимать, что любые действия персонала, как умышленные, так и непреднамеренные, в подавляющем большинстве случаев обусловлены невыполнением требований к нормативной деятельности. Это в первую очередь нарушения должностных инструкций, квалификационных требований, стандартов и графиков выполнения работы, административных регламентов, пропускного режима и прочих директивных требований к обеспечению безопасности объекта и организации работы персонала.

Полученные в результате инспекционных проверок данные служат основанием для определения количественных оценок степени доверия к надежности (качеству) выполнения персоналом объекта своих функций. Вообще доверие по отношению к личности играет формообразующую роль [16]. Потеря доверия — это потеря лица. В. П. Зинченко показал, что доверие — (любое: к общему порядку вещей, к коллективу или к самому себе) в основной своей части относится к эмоциональной сфере психики, что оно способно порождать многие чувства и установки (от принятия до отторжения), что, вернув доверие, получаешь только шанс, но не гарантию его восстановления. Доверие теснейшим образом связано с культурой личности и межличностных отношений. Одно из практических следствий психологического понимания доверия состоит в том, что непозволительно смешивать доверие к личностным качествам с доверием к социальному статусу человека или к организации в целом.

Нормативную базу для оценок степени доверия должны составлять стандартные «таблицы оценки степени доверия», отражающие зависимость степени доверия от количества различных нарушений, выявленных в результате инспекционных проверок. Стандартные таблицы оценки степени доверия должны быть разработаны в результате специальной

**Таблица 1**

Стандартная таблица оценки степени доверия к персоналу

| № нарушения – i | Нарушения и оценки по результатам инспекции | Число нарушений за контрольный период | Степень доверия $D_i$ |
|---|---|---|---|
| 1 | Факты умышленных и противоправных действий, совершенных неопределенным членом персонала; действия инсайдеров | 1 | 0,5 |
| | | 2 | 0.3 |
| | | Больше 2-х | 0 |
| 2 | Нарушения нормативной деятельности (пропускного режима, трудовой дисциплины, отчетности и т. п.) | 1 | 0,95 |
| | | 2 | 0,9 |
| | | Более 2-х | 0,8 |
| 3 | Непреднамеренные ошибки | 1 | 0,85 |
| | | 2 | 0,7 |
| | | Более 2-х | 0,6 |
| 4 | Средняя оценка профессиональной подготовки персонала (здесь и ниже по условной пятибалльной шкале) | 5 | 1 |
| | | 4 | 0,95 |
| | | 3 | 0,8 |
| | | Ниже 3-х | 0,1 |
| 5 | Оценка слаженности действий в чрезвычайных ситуациях | 5 | 1 |
| | | 4 | 0,9 |
| | | 3 | 0,5 |
| | | Ниже 3-х | 0,1 |
| 6 | Оценка действий руководства | 5 | 1 |
| | | 4 | 0,9 |
| | | 3 | 0, 7 |
| | | Ниже 3-х | 0,1 |

научно-исследовательской работы с привлечением экспертов-практиков и утверждены установленным порядком[17].

Таблицы оценки степени доверия должны содержать стандартный набор видов нарушений и соответствующий каждому виду нарушений показатель степени доверия, как, например, в гипотетической табл. 1.

Степень доверия определяется путем сравнения показателей нарушений и данных инспекционных проверок, хранящихся в базе данных, со стандартными таблицами оценки степени доверия [17].

Взаимосвязь степени доверия и величины риска по обнаруженным нарушениям определяется с помощью гипотетической табл. 2.

**Таблица 2**

| Номер нарушения $i$ | Степень доверия $D_i$ | Весовой коэффициент $b_i$ | Величина риска $P_i$ |
|---|---|---|---|
| 1 | 0.9 | 1 | 0,1 |
| 2 | 0.6 | 0,8 | 0,32 |
| 3 | 0.8 | 0,6 | 0,12 |
| …. | …. | …. | |

Величина риска $P_i$ по каждому $i$-му нарушению определяется [17] по формуле

$$(1 - D_i) * b_i = P_i, \qquad (1),$$

где $D_i$ — степень доверия по $i$-му нарушению, $b_i$ — весовой коэффициент, определяющий степень влияния $i$-го нарушения на общую оценку доверия к персоналу.

Расчет суммарного риска нарушения безопасности объекта транспортной инфраструктуры в результате нарушений в работе персонала производится по формуле (2)

$$P_{сум} = 1 - \prod_{i=1}^{I} [1 - P_i]. \qquad (2)$$

Разработка стандартных таблиц степени доверия предполагает также определение критической величины, именуемой **«допустимая степень доверия».** Если степень доверия к персоналу какого-либо инспектируемого объекта оказывается меньше допустимой степени доверия, то этой структуре доверять нельзя и необходимо предпринять срочные организационные, кадровые, финансовые и другие меры для исправления опасной ситуации.

## Литература


1. *Коваль Е. А*. [Электронный ресурс] www. cyberleninka. Ru/ article/
2. *Либерман А. Н.* Техногенная безопасность: человеческий фактор. Спб,, 2006.
3. *Цыгичко В. Н*., *Черешкин Д. С*. Безопасность критически важных объектов транспортного комплекса. М.: URSS, 2014.
4. Федеральный закон о транспортной безопасности ФЗ 16 (ред. 03.02 20142014).
5. Безопасность транспорта. // в кн. Горизонты промышленной политики. М., 2003: www.prompolit.ru (89723).
6. *Ольшанский Д. В*. Психология терроризма. Спб.: Питер, 2002.
7. *Агатова Л. А*., *Смолян Г. Л*., *Солнцева Г. Н.* Нелояльность персонала как угроза безопасности организации // Труды ИСА РАН. 2007. Т. 31. С. 216–230.
8. *Староверов Д. А*. Лояльность персонала как фактор безопасности бизнеса // [Электронный ресурс] www/amulet-group.ru/page..id?htm=
9. *Горностаев С. В*. Нематериальные факторы, влияющие нам уровень лояльности персонала// Управление человеческим потенциалом. 2005. №3.
10. *Новицкий Е. Г*. Управление рисками информационной безопасности в крупных диверсифицированных корпорациях // Препринт, ИСА РАН, 1999.
11. *Вершинин Михаил*. Современные молодежные субкультуры: хакеры // [Электронный ресурс] www.psyfactor.org/lib/vershinin 4.htm
12. *Смолян Г. Л*., *Солнцева Г. Н*. Непреднамеренные ошибки людей как угроза безопасности организационных систем // Труды ИСА РАН. 2010. Т. 52 С. 152–164.
13. *Костюк В. Н*. Информация как социальный и экономический ресурс. М., 1997.
14. Справочник по .прикладной эргономике. М., 1980.
15. *Мунипов В. М., Зинченко В. П*. Эргономика. Человекоориентированное проектирование техники, программных средств и среды. М.: Логос, 2001.
16. *Зинченко В. П.* Доверие. Большой психологический словарь. М.: АСТ, 2009.
17. *Кононов А. А*., *Стиславский А. Б.*, *Цыгичко В. Н*. Управление рисками нарушения транспортной безопасности. М.: АС-Траст, 2008.


**Смолян Георгий Львович.** Гл. н. с. ИСА РАН. Д. философ. н. Окончил в 1952 г. МГУ. Количество печатных работ: 170, в т. ч. 3 монографии. Область научных интересов: социальные и психологические проблемы автоматизации управления. E-mail: smolyan2013@mail.ru

**Солнцева Галина Николаевна**. Доцент факультета психологии МГУ. К. психол. н. Окончила в 1971 г. МГУ. Количество печатных работ: 75, в т. ч. 3 монографии. Область научных интересов: инженерная психология, теория принятия решения, структура и регуляция деятельности. E-mail: galinasolntseva@mail.ru