ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРОМЫШЛЕННОМУ РАЗВИТИЮ

Обеспечение промышленной безопасности и охраны труда

СПРАВОЧНИК

- Организация Объединенных Наций по промышленному развитию
- Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор)
- Британский институт стандартов

РУССКИЙ

ВСЕОБЩЕЕ УСТОЙЧИВОЕ ПРОМЫШЛЕННОЕ РАЗВИТИЕ

Обеспечение промышленной безопасности и охраны труда

Справочник

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ПРОМЫШЛЕННОМУ РАЗВИТИЮ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ (РОСТЕХНАДЗОР)

БРИТАНСКИЙ ИНСТИТУТ СТАНДАРТОВ

Вена (Австрия)
Август 2021 года

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРОМЫШЛЕННОМУ РАЗВИТИЮ

www.unido.org

БЛАГОДАРНОСТЬ

Этот справочник был подготовлен в рамках проекта ЮНИДО «Обеспечение промышленной безопасности и охраны труда», который финансируется Российской Федерацией, и является плодом сотрудничества между Организацией Объединенных Наций по промышленному развитию (ЮНИДО), Ростехнадзором (Федеральной службой по экологическому, технологическому и атомному надзору) и BSI (Британским институтом стандартов), которые работали под общим руководством специалиста по промышленному развитию ЮНИДО Фаррухбека Алимджанова. Руководитель направления охраны здоровья, безопасности труда и благополучия BSI Global Кейт Филд предоставила модели и ценные материалы. Большой вклад в эту работу внесли генеральный директор компании Acuizen Technologies ДжСи Секар и управляющий партнер компании Clyde&Co (Австралия) Майкл Тоома. Младшие сотрудники проекта Оливер Отрид и Йана Роэссл предоставили дополнительные исходные данные и материалы, вошедшие в этот справочник.

Нам хотелось бы высказать особую благодарность начальнику управления международного сотрудничества и протокола Ростехнадзора Ирине Викторовне Соколовой за неизменную поддержку, ценные комментарии и замечания, а также за координацию усилий на протяжении всего проекта совместно с заместителем начальника управления международного сотрудничества и протокола Дмитрием Владимировичем Чачеловым.

Кроме того, мы очень признательны и благодарны Кейт Филд за неизменную поддержку и предоставление экспертной оценки в ходе всех работ по проекту, Майклу Тоома, ДжСи Секару и другим специалистам, которые принимали участие в цикле вебинаров и конференциях. Результаты этого проекта, включая доклад на Конференции по обеспечению промышленной безопасности и охраны труда, теоретические модели и исследования, часто упоминаются в этом справочнике и служат основой для последующих выводов.

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ

Оглавление

Введение

Повышение осведомленности в сфере промышленной безопасности, особенно в сфере охраны труда и техники безопасности (ОТ и ТБ) на местном (организация), национальном, региональном и международном уровнях — первый шаг к обеспечению промышленной безопасности. Многие организации и национальные правительства (даже в промышленно развитых регионах) не осознают критическую значимость промышленной безопасности, либо пытаются не придавать этому значения.

Проект ЮНИДО «Обеспечение промышленной безопасности и охраны труда» был реализован в рамках сотрудничества ЮНИДО и Ростехнадзора (Федеральной службы по экологическому, технологическому и атомному надзору) и подчеркнул необходимость безотлагательного решения целого ряда вопросов, касающихся безопасности. В конце мая 2019 года в Вене состоялась первая Международная конференция по обеспечению промышленной безопасности и охраны труда, ставшая частью кампании по повышению осведомленности и призванная распространять передовой опыт в сфере промышленной безопасности. Она стала ярким примером вложения сил и средств в обеспечение промышленной безопасности во всех странах, чтобы никто не остался позади. Впоследствии и в ответ на пандемию COVID-19, ЮНИДО и Ростехнадзор организовали цикл вебинаров, в ходе которых рассматривались вопросы, связанные со всеми аспектами безопасности, и прежде всего наиболее актуальные вопросы с точки зрения меняющихся на фоне пандемии условий. Будучи еще одной отправной точкой, этот справочник дает определенное представление о некоторых требованиях к обеспечению безопасной рабочей среды и опирается на самые современные международные компетенции.

Повышение осведомленности в сфере промышленной безопасности, особенно в сфере охраны труда и техники безопасности (ОТ и ТБ) на местном (организация), национальном, региональном и международном уровнях — первый шаг к обеспечению промышленной безопасности. Многие организации и национальные правительства (даже в промышленно развитых регионах) не осознают критическую значимость промышленной безопасности, либо пытаются не придавать этому значения.

По данным МОТ, в мире ежедневно более 6500 человек умирают от заболеваний, связанных с производством, и свыше 1000 человек погибают в результате несчастных случаев на производстве[1]. Ежегодное количество смертей, связанных с производством, возросло с 2,33 млн в 2014 году до 2,78 млн в 2017 году[2]. Из 2,78 млн связанных с производством смертей, которые были зафиксированы в 2017 году, 2,4 млн были связаны с профессиональными заболеваниями[3]. Максимальная доля несчастных случаев на производстве со смертельным исходом приходится на Азию (71,5% в 2014 году), затем идет Африка (18,9%), Америка (6,5%) и Европа (2,9%)[4]. Наиболее высокая смертность от несчастных случаев на 100 000 человек наблюдалась в Африке (17,4) и Азии (13,0), что отражает глобальное распределение занятого населения и опасных работ, а также различия в уровнях экономического развития.

Источником производственных рисков, несчастных случаев на производстве и заболеваний, связанных с производством, могут становиться технологические или промышленные условия, опасные процедуры, сбои на уровне инфраструктуры или определенные действия людей.[5] Они могут оказывать

1) МОТ, 2019 год
2) Hämäläinen, Takala и Boon Kiat, 2017 год
3) Hämäläinen, Takala и Boon Kiat, 2017 год
4) Hämäläinen, Takala и Boon Kiat, 2017 год
5) МОТ, 2019 год

значительное влияние не только на работников, но и на их семьи и общество в целом как в краткосрочной, так и в долгосрочной перспективе посредством травм или гибели людей, ухудшения здоровья, когнитивных функций и эмоционального благополучия, социальной и экономической дестабилизации, имущественного ущерба и ухудшения экологической ситуации. Кроме того, подобные риски могут снижать производительность и эффективность предприятий за счет дезорганизации производства, ухудшения конкурентоспособности и репутационных потерь предприятий по всем цепочкам поставок и в целом отрицательно сказываться на состоянии экономики и общества.

Промышленная безопасность включает в себя предотвращение широкого спектра производственных рисков, несчастных случаев на производстве и заболеваний, связанных с производством, в целях создания среды с нулевым риском. Хотя создание подобной среды следует рассматривать как сверхзадачу, эффективные стратегии предотвращения на уровне предприятия, страны, региона и на глобальном уровне могут устранить риски или хотя бы свести их к минимуму.

Поскольку в производственной деятельности невозможно полностью исключить риски, вызываемые природными явлениями и человеком, очень важно как можно лучше понять характер этих рисков, чтобы донести эту информацию до надзорных органов и принять действенные меры по смягчению рисков, используя передовые практики и лучшие доступные технологии[6].

Для обеспечения эффективной охраны окружающей среды и исключения потенциальных производственных рисков, несчастных случаев и опасных факторов необходимы согласованные действия как на международном, так и на национальном уровне. На международном уровне управление негативными воздействиями в результате несчастных случаев на производстве осуществляется с помощью протоколов, конвенций и соглашений. Сотрудничество между коммерческими организациями, гражданским обществом и государственными органами также является совершенно необходимым для обмена критически важной информацией и обеспечения приверженности одним и тем же целям[7].

В этом справочнике рассматриваются основополагающие концепции обеспечения промышленной безопасности и охраны труда. В нем также содержится информация о современных тенденциях в сфере управления промышленной безопасностью, включая организационные аспекты (особенно в свете пандемии COVID-19 и вызванной ею дестабилизации), в сфере технологической безопасности, а также рассматриваются важные вопросы кибербезопасности.

Кибербезопасность играет ключевую роль в современной производственной среде и требует ответственного подхода с самого начала. Удаленная работа выявила уязвимости в организациях и компаниях. Прочие тенденции цифровизации и объединение производственного оборудования в единую систему демонстрируют всё возрастающую роль кибербезопасности и комплексного подхода к вопросам промышленной безопасности и охраны труда, который использован в этом справочнике.

6) ЮНИДО, 2019 год
7) ЮНИДО, 2019 год

Устойчивость организации к внешним воздействиям

1

Даже в организациях, где имелись планы непрерывности бизнеса, которые учитывали риск пандемии, невозможно было предусмотреть тяжесть последствий эпидемии COVID-19. Неудивительно, что существующие подходы к управлению рисками часто не соответствовали обстановке. Это очень четко прослеживалось в сфере промышленной безопасности: был зафиксирован рост числа несчастных случаев, особенно при вводе оборудования в эксплуатацию после периодов обязательной «самоизоляции» (требований оставаться дома, чтобы поставить под контроль распространение эпидемии COVID-19). Это также прослеживалось в сфере охраны труда и техники безопасности по мере того, как организации старались наладить управление психосоциальными рисками, связанными с пандемией (например, риск изоляции при работе из дома).

Центральным элементом промышленной безопасности является эффективное управление рисками. Речь идет о скоординированном наборе действий, осуществляемых людьми определенным образом с целью управления неопределенностью[8]. Кроме того, управление рисками регулирует любое число других бизнес-процессов, включая финансы и качество. Эти подходы к управлению рисками носят преимущественно защитный характер: они нацелены на предотвращение «плохих» событий и в общих чертах оправдывают ожидания. Проблема возникает в тот момент, когда в результате непредвиденного изменения требуется подвижность и гибкость.

Это стало особенно актуально в течение 2020 года, когда новый коронавирус SARS-CoV-2 вызвал пандемию COVID-19. Даже в организациях, где имелись планы непрерывности бизнеса, которые учитывали риск пандемии, невозможно было предусмотреть тяжесть последствий эпидемии COVID-19. Неудивительно, что существующие подходы к управлению рисками часто не соответствовали обстановке. Это очень четко прослеживалось в сфере промышленной безопасности: был зафиксирован рост числа несчастных случаев, особенно при вводе оборудования в эксплуатацию после периодов обязательной «самоизоляции» (требований оставаться дома, чтобы поставить под контроль распространение эпидемии COVID-19).

Рис. 1. Устойчивость организации к внешним воздействиям — «Квадрант напряжений»

8) Сформулировано на основе стандарта BS 31100:2011

Это также прослеживалось в сфере охраны труда и техники безопасности по мере того, как организации старались наладить управление психосоциальными рисками, связанными с пандемией (например риск изоляции при работе из дома).

В ответ на пандемию в центре внимания вновь оказалось понятие «устойчивость организации к внешним воздействиям». Устойчивость организации к внешним воздействиям — это «способность организации предугадывать поэтапные изменения и внезапную дестабилизацию, готовиться к ним, реагировать на них и адаптироваться к ним, чтобы остаться на рынке и преуспеть»[9]. Устойчивость организации к внешним воздействиям предполагает более комплексный и упреждающий подход к управлению рисками за счет выявления различных аспектов лидерского поведения и организационного потенциала, которые необходимы, чтобы благополучно пережить период турбулентности. Стратегический инструмент оценки напряжений (см. иллюстрацию на соседней странице[10]) отражает баланс между защитными (предотвратить «плохие» события) и поступательными (добиться желаемых результатов) действиями, нацеленными на результат, тогда как подвижность достигается за счет баланса между постоянством и гибкостью.

Лидерам, стремящимся обеспечить устойчивость к внешним воздействиям, нужно определить оптимальный баланс четырех типов поведения, что иногда влечет за собой контринтуитивные решения.

Защитный угол зрения, который нацелен на избегание убытков и сохранение стоимости. Это — превентивный контроль (защитный подход и постоянство) и осознанные действия (защитный подход и гибкость). Сюда следует отнести управление рисками и планирование непрерывности бизнеса.

Подвижный угол зрения, который нацелен на возможности и рост. Это — оптимизация производительности (поступательный подход и постоянство) и адаптивные инновации (поступательный подход и гибкость). В этом суть устойчивости организации к внешним воздействиям.

9) Определение из стандарта BS 65000:2014 «Руководство по устойчивости организации к внешним воздействиям»

10) Denyer, D. (2017 год). Organizational Resilience: A summary of academic evidence, business insights and new thinking/Устойчивость организации к внешним воздействиям: научные доказательства, практические знания и новое мышление (краткое изложение) BSI and Cranfield School of Management

Устойчивость организации к внешним воздействиям — это не одноразовое мероприятие. Для обеспечения и повышения устойчивости требуется постоянная оценка и непрерывный мониторинг как внутренних, так и внешних факторов. Управление устойчивостью организации к внешним воздействиям требует использования передовых методов для непрерывного совершенствования бизнеса за счет выстраивания компетенций и накопления потенциала во всех подразделениях организации. Чтобы помочь организациям лучше понять, в чем заключается устойчивость к внешним воздействиям, BSI подготовил комплекс передовых методов, который позволит организациям ознакомиться с ключевыми элементами, нужными для обеспечения высокой устойчивости к внешним воздействиям.

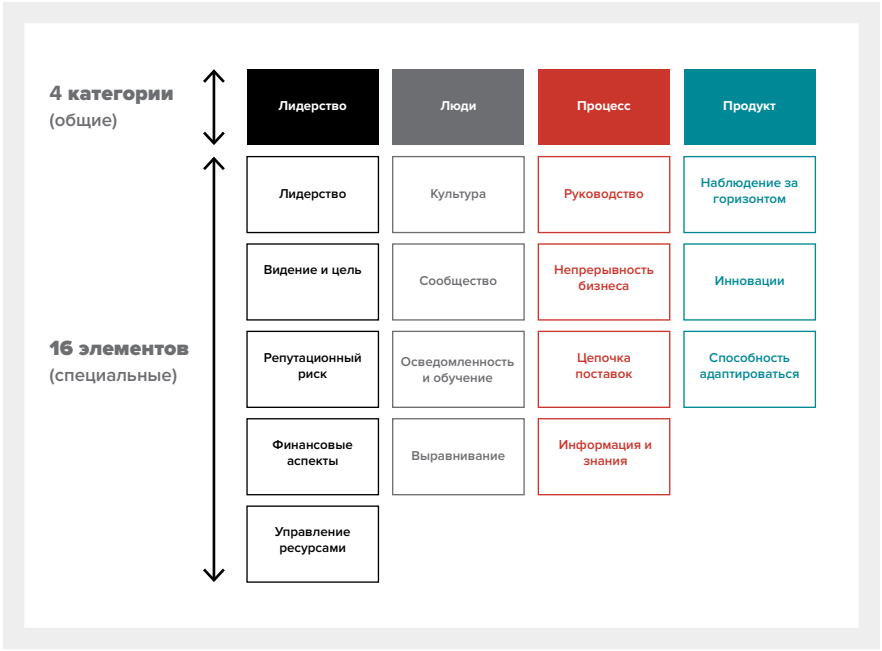


Рис. 2. Матрица BSI «Устойчивость организации к внешним воздействиям»

Матрица состоит из четырех ключевых категорий, под которыми расположены шестнадцать специальных элементов. Лидерство подразумевает подотчетность заинтересованным лицам и ответственность перед ними за высокую устойчивость организации к внешним воздействиям и ее процветание в долгосрочной перспективе. Именно лидерство определяет, каким образом взаимодействуют и насколько успешны другие категории. Вот почему эффективное лидерство является критическим фактором успеха.

ЛИДЕРСТВО

1. **Лидерство** — Культура, заметность и результаты высшего руководства организации.
2. **Видение и цель** — Каким образом цель определяется, доводится до сведения и относится к распределению стратегических ресурсов.
3. **Репутационный риск** — Подход бизнеса к управлению репутационным риском и его ограничению.
4. **Финансовые аспекты** — Качество управления финансовыми аспектами бизнеса.
5. **Управление ресурсами** — Насколько эффективно осуществляется управление ресурсами (людьми и технологиями) с точки зрения их развертывания в случае необходимости.

ЛЮДИ

6. **Культура** — В какой степени сотрудники разделяют ценности и поведенческие стратегии, насколько сильны доверие и мотивация сотрудников.
7. **Сообщество** — Отношения в бизнес-сообществе, ответственное планирование и управление, социальная ответственность
8. **Осведомленность, обучение и тестирование** — Уровни осведомленности, обучения и тестирования устойчивости организации к внешним воздействиям
9. **Выравнивание** — Насколько все аспекты организации, включая качество, охрану труда, технику безопасности и информационную безопасность, соотносятся с реализуемой стратегией.

ПРОЦЕСС

10. **Руководство** — Насколько четко определены принципы управления и в какой степени высшее руководство организации подотчетно всем заинтересованным лицам
11. **Непрерывность бизнеса** — Качество принципов, политик и процедур, касающихся непрерывности бизнеса
12. **Цепочка поставок** — Качество управления цепочкой поставок, безопасность и управление
13. **Информация и знания** — Качество информационных ресурсов и обмен знаниями

ПРОДУКТ

14. **Наблюдение за горизонтом** — Насколько системно бизнес изучает информацию, чтобы выявлять изменения, угрозы, риски и возможности
15. **Инновации** — Насколько корпоративная культура стимулирует и поощряет инновации
16. **Способность адаптироваться** — Способность выявлять изменения и неопределенность, а также оперативно предпринимать эффективные действия

2

Модель 3C-3P устойчивой системы промышленной безопасности

Ни в коем случае не следует думать, будто события, которые влекут за собой дестабилизацию промышленности (подобные пандемии COVID-19), больше не повторятся. Мы всё яснее понимаем, что живем в мире, где «шоки» будут возникать вновь и вновь. Поскольку мы живем во взаимосвязанном и взаимозависимом мире, эти шоки могут возникать где угодно, принимать самые разные формы и дестабилизировать виды деятельности, которые, на первый взгляд, никак не связаны друг с другом. «Устойчивость к внешним воздействиям» — это про нашу способность к восстановлению не если случится шок, а когда случится шок.

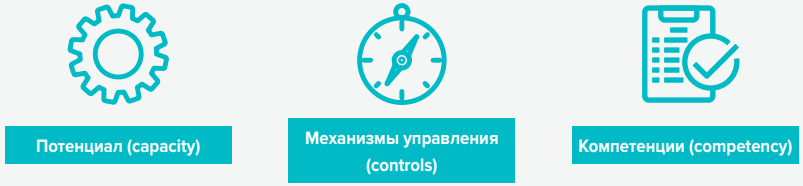
УСТОЙЧИВОСТЬ К ВНЕШНИМ ВОЗДЕЙСТВИЯМ И ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ

На первый взгляд, устойчивость к внешним воздействиям в контексте промышленной безопасности сводится к нашей способности «безопасно» вернуться в исходное состояние. Обычно мы воспринимаем понятие «безопасный» как отсутствие неожиданных происшествий. Тем не менее, важно признать, что отсутствие происшествий — лишь запаздывающий показатель. Он не обязательно отражает аспекты, которые обеспечивают безопасность системы и повышают ее устойчивость к внешним воздействиям.

Эти «аспекты», обеспечивающие безопасность системы и ее устойчивость к внешним воздействиям, следует включать во все определения термина «безопасность». При таком подходе акцент будет смещаться с «отсутствия» происшествий на «наличие» таких проверок.

БЕЗОПАСНОСТЬ И ЭЛЕМЕНТЫ 3-С

Представляются важными три аспекта, которые позволяют сформулировать более точное определение безопасности. Речь идет о так называемых элементах 3-С:



Потенциал

Несомненно, важнейшим требованием к любой системе, устойчивой к внешним воздействиям, является качество «потенциала», который позволяет выстоять в шоковой ситуации. Его можно разбить на две категории:

ПРОФЕССИОНАЛЬНЫЙ ПОТЕНЦИАЛ

Речь идет о наличии у организации достаточных ресурсов — от финансов и оборудования до материалов и технологий. Причем рассматривается не только само существование этих ресурсов, но и изменения, которым может подвергаться каждый из этих факторов в случае шока. Несчастные случаи и происшествия происходят вследствие того или иного опасного энергетического воздействия, а наличие **материального потенциала** обеспечивает поглощение этой энергии таким образом, который исключает негативные последствия.

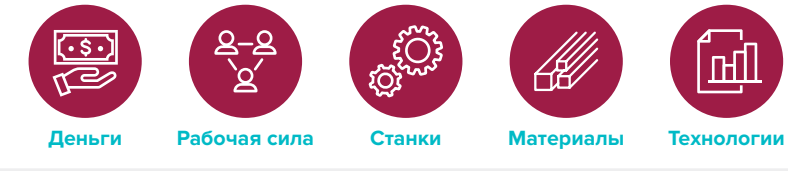


Рис. 3. © Acuizen Technologies

ЧЕЛОВЕЧЕСКИЙ ПОТЕНЦИАЛ

В то время как «материальный» потенциал может играть ключевую роль в содействии восстановлению организации, нельзя недооценивать важность «человеческого» потенциала. Речь идет о таких аспектах, как культура организации. Эти аспекты включают уровень доверия и уважения, которые испытывают друг к другу руководство и низовые звенья организации. В ситуациях, подобных нынешней пандемии, у руководства есть прекрасная возможность проявить столь необходимое участие к работникам и завоевать их доверие, необходимое для выстраивания гармоничных долгосрочных отношений.

Еще одним показателем человеческого потенциала является то, насколько организации удалось встроить своих сотрудников в «образовательную среду». Считается, что наш мир становится всё более изменчивым, неопределенным, сложным и неоднозначным. Организациям необходимо принять эту непредсказуемость как новую нормальность и готовить свой персонал к эффективной работе в подобных условиях. Для этого необходимо создать среду, где обучение является динамичным и непрерывным — еще один показатель устойчивости к внешним воздействиям.

Организациям понадобится приложить целенаправленные усилия, чтобы измерить свой «материальный» и «человеческий» потенциал, а также чтобы управлять ими. Эти усилия могут принимать различные формы, включая, среди прочего, анализ проектных решений, исследования путем моделирования, «настольные» учения и опросы. Это — стремительно развивающаяся область исследований. Нам предстоит еще многое сделать, чтобы подобрать правильные показатели.

Механизмы управления

Исходя из нашего общего представления об управлении рисками, мы воспринимаем его как наличие опасности и порождающего фактора (в том числе внешнего воздействия или неуместного действия, которое потенциально может вызвать происшествие). Представляется важным определить вероятность порождающего фактора, поскольку само по себе наличие опасности не обязательно означает, что она перерастет в происшествие или несчастный случай. Это происшествие может иметь незначительные или потенциально значительные последствия — например, повлечь за собой гибель людей. Для измерения последствий используется параметр тяжести.

Рис. 4. © Acuizen Technologies

Как правило, для осознания риска мы рассматриваем события с точки зрения сочетания вероятности и тяжести, которые измеряются с помощью различных количественных и качественных методов.

В идеале, опасные факторы следует исключить полностью. Но существуют несколько практических соображений и неизвестных явлений, из-за которых определенная степень риска в нашей жизни является неизбежной. Тем не менее, мы можем значительно снизить риски, применяя механизмы управления на различных этапах. Речь идет о типичной структуре механизмов управления в диапазоне от устранения, замены, комплексного проектирования и руководства до средств индивидуальной защиты (СИЗ). Смысл этих механизмов управления заключается в том, чтобы устранить опасность (в идеале), либо, как минимум, уберечь человека от вреда, если опасность выразится в реализации риска.

Организациям требуется осознать необходимость в механизмах управления и необходимость их существования для всех потенциальных опасностей.

Компетенции

Центральное место в любой деятельности занимает человек. Именно человеческие знания и навыки упрощают осуществление любой деятельности. Даже когда деятельность автоматизирована, в конечном счете качество ее исполнения определяется навыками человека, который программировал и разрабатывал процесс.

Безусловно, одним из первых шагов является формальное (очное) или неформальное (иным способом) обучение людей выполнению задач. Тем не менее, единичный учебный курс не дает гарантий того, что человек приобрел компетенции, необходимые для выполнения порученной задачи.

Компетенции выстраиваются с течением времени и с появлением опыта. Например, для развития сотрудника важна структура, в рамках которой он осуществляет все шаги, связанные с его трудовой деятельностью. При этом главным фактором успеха, конечно же, является умение мотивировать человека, привить ему правильное отношение, а также способность человека постоянно поддерживать существующие навыки, совершенствовать их и приобретать новые.

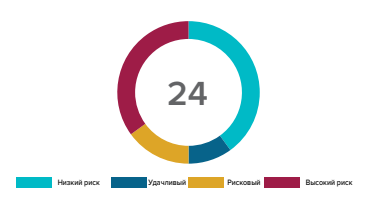
Рис. 5. Спираль компетенций AcuiZen

КОМПЕТЕНТНОСТЬ В ОБЛАСТИ РИСКОВ

Если рассматривать понятие «компетентность» в контексте безопасности, необходимо измерить «компетентность в области рисков» как на функциональном, так и на индивидуальном уровне. Наличие компетентности в области рисков указывает, в какой степени организация и ее сотрудники способны распознавать риски и своевременно реагировать на них.

Существуют алгоритмизированные механизмы, которые оценивают компетентность в области рисков отдельного человека и крупных функциональных подразделений в составе организации. Исходя из ответов на ряд вопросов, индекс определяет профиль риска конкретного человека и относит его к четко определенной категории.

Рис. 6. © Acuizen Technologies



Алгоритм рассчитывает профиль риска для конкретного человека, функционального подразделения и организации в целом. Пример такого расчета приведен слева.

ПОВТОРНАЯ АКТИВАЦИЯ

В динамичном мире со множеством источников информации (и дезинформации) не так уж сложно упустить из виду некоторые фундаментальные принципы обеспечения безопасности. Подобная оплошность может дорого обойтись с точки зрения результатов в области безопасности. Систематическое подкрепление этих базовых принципов является критически значимым шагом в обеспечении компетентности.

Например, компания AcuiZen продемонстрировала важную роль технологии при измерении компетенций работников на основе того, насколько хорошо они усвоили базовые понятия безопасности. Индекс также измеряет уровень вовлечения работника, подготавливая почву для вмешательства человека там, где это необходимо.

СОЦИАЛЬНЫЕ КОМПЕТЕНЦИИ

В мире, где технологии успешно вытесняют ручной труд, нельзя недооценивать необходимость вырабатывать больше социальных навыков в ходе взаимодействия между людьми. С точки зрения безопасности не менее важно располагать механизмом раннего обнаружения социально-психологических факторов, которые могут поставить под угрозу безопасность людей и процессов. Не выявленный психологический стресс и другие факторы, влияющие на благополучие работников, могут стать причиной серьезных происшествий.

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ЭЛЕМЕНТОВ 3-С

Элементы 3-С лежат в основе определения устойчивой системы промышленной безопасности и требований к ней. Как реализовать эти элементы на практике?

Возможно, ответ на этот вопрос следует искать в Концепции нулевого видения.

Концепция нулевого видения

Концепция нулевого видения — всемирная инициатива, осуществляемая с 2015 года. Приверженцы этой стремительно разрастающейся инициативы призывают всех — служащих, рабочих, профсоюзы и государственные органы — проявить сознательность и воплотить в жизнь ее главный принцип: все производственные травмы и происшествия, ухудшающие здоровье, можно предотвратить. Ведь если приложить усилия, нулевой травматизм может стать вполне реальным сценарием.

Концепция нулевого видения предполагает согласованный комплексный подход, который обеспечит учет всех видов опасных факторов и осуществление действий, способных смягчить риски. Природа опасностей может различаться в зависимости от специфики конкретной организации. Тем не менее, мы можем получить достоверную общую картину, рассмотрев системы безопасности с точки зрения людей, производственного процесса и продукции.

БЕЗОПАСНОСТЬ ЛЮДЕЙ

Безопасность людей обеспечивает охрана труда и техника безопасности (ОТ и ТБ) — междисциплинарная область, которая занимается вопросами безопасности, охраны здоровья и благополучия **людей** на производстве. Для организаций хорошей отправной точкой может стать изучение стандартов (например ISO 45001 «Системы менеджмента безопасности труда и охраны здоровья» и дополняющий его стандарт ISO 45003 «Системы менеджмента безопасности труда и охраны здоровья. Психологическое здоровье и безопасность на рабочем месте. Руководство по применению»), которые предоставляют нормативную базу для создания условий труда, более безопасных для физического и психического здоровья персонала.

БЕЗОПАСНОСТЬ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА

Безопасность производственного процесса обычно ассоциируется с производствами, где используются опасные материалы, в том числе нефтеперерабатывающими заводами, нефте- и газодобывающими предприятиями, а также предприятиями химической промышленности. Они сосредотачивают усилия на предотвращении пожаров, взрывов и аварийных выбросов химических веществ.

Безопасность производственного процесса во многих случаях является нормативным требованием. Различные юрисдикции по-разному подходят к регулированию безопасности производственных процессов. Приведем в качестве примера систему управления безопасностью производственного процесса (УБПП) — нормативный документ, распространяемый Управлением охраны труда и техники безопасности США (OSHA).

По-видимому, общие принципы УБПП разработаны для производств, где используются опасные материалы. Тем не менее, основные принципы УБПП, вероятно, можно адаптировать и применять ко всем видам производственной деятельности.

БЕЗОПАСНОСТЬ ПРОДУКЦИИ

Термин «**безопасность продукции**» используется для описания политик, которые разработаны для защиты людей от рисков, связанных с тысячами потребительских товаров, которые они приобретают и используют ежедневно. С точки зрения промышленного производства он будет включать оборудование, эксплуатация которого осуществляется в рамках процессов.

В большинстве случаев безопасность продукции также является предметом регулирования. Например, в Европе Регламент по безопасности электрооборудования и Директива 2014/35/EU о низковольтном оборудовании распространяются на большую часть электрооборудования, используемого в быту, в офисе и в промышленности. Директива о низковольтном оборудовании / Регламент по безопасности электрооборудования предусматривают, что электрооборудование поступает в продажу только в том случае, если оно не представляет опасности для людей, имущества и домашних животных.

Заверения о безопасности продукции должны подтверждаться соблюдением применимых нормативных требований и знаками омологации / сертификации, включая знак CE, знак UKCA, знак Kitemark BSI и знак безопасности UL.

Говоря об устойчивой и безопасной системе, следует остановиться подробнее на всех этих трех составляющих безопасности. В реальности все эти сферы частично накладываются друг на друга и являются взаимозависимыми. На иллюстрации ниже изображена подобная система с частичным наложением.

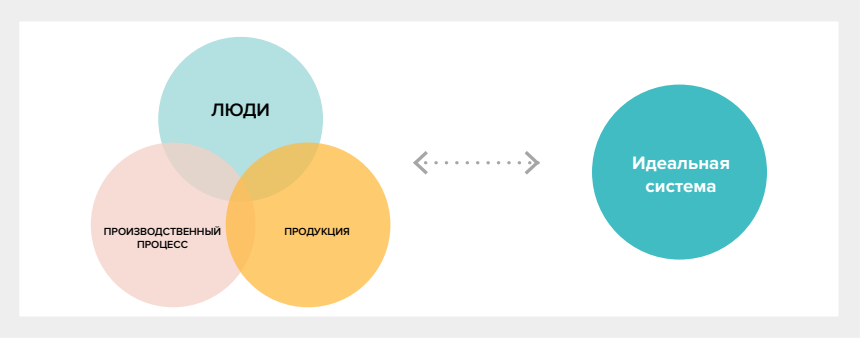


Рис. 6. Визуальное представление трех составляющих безопасности в устойчивой и безопасной системе

Зоны наложения указывают на сегменты, где необходимо выстроить надежные системы, охватывающие все три аспекта (центральная часть). Также существуют зоны наложения, которые охватывают два аспекта. На остальных участках доминирует один аспект. Возможно, это свидетельствует о недостаточном внимании к двум другим аспектам.

В идеальной системе все эти три аспекта глубоко интегрированы и всесторонне охвачены. Поэтому их наложение дает одну окружность (см. правую часть рис. 6).

Эта окружность представляет собой тот самый нуль и напоминает о том, что нулевое видение возможно, если использовать комплексный подход и уделять достаточное внимание всем элементам 3-Р (люди, производственный процесс, продукция).

Учитывая динамичный характер современных производственных операций, достижение «нулевого травматизма» станет постоянной целью. Следует ожидать появления новых дестабилизирующих событий, которые выявят уязвимости в безопасности людей, производственного процесса или продукции. Организациям необходимо прилагать целенаправленные усилия для выявления этих дестабилизирующих событий и устранения уязвимостей с помощью эффективных действий технического или административного характера. Это должен быть непрерывный и динамичный процесс.

В такой ситуации одним из определяющих факторов организации, устойчивой к внешним воздействиям, может стать способность оперативно взаимодействовать с заинтересованными лицами в ходе подобных дестабилизирующих событий, а также сотрудничать и действовать сообразно обстоятельствам.

Культура безопасности

3

Культура организации оперирует такими понятиями, как «ценности, отношения, управленческие практики, восприятия, компетенции и закономерности деятельности на уровне отдельного человека и группы», и, соответственно, влияет на все аспекты организации. Вот почему в матрице устойчивости к внешним воздействиям культура отнесена к категории «Люди». Вместо слова «культура» часто говорят «здесь так принято» или «ДНК организации».

Термин «культура безопасности» получил широкое распространение после того, как был упомянут в качестве первопричины аварии на Чернобыльской АЭС. Консультативная группа по безопасности Международного агентства по атомной энергии предложила следующее определение:

«... продукт индивидуальных и групповых ценностей, отношений, компетенций и поведенческих сценариев, которые определяют приверженность программам охраны труда и техники безопасности организации, а также их стилистику и профессиональные навыки в этой сфере».

Хотя это определение было продиктовано требованиями промышленной безопасности, если организация просто сосредоточится на одном из аспектов культуры (в данном случае – безопасности), то она упустит самое главное. Культура организации оперирует такими понятиями, как «ценности, отношения, управленческие практики, восприятия, компетенции и закономерности деятельности на уровне отдельного человека и группы»[11] и, соответственно, влияет на все аспекты организации. Вот почему в матрице устойчивости к внешним воздействиям культура отнесена к категории «Люди». Вместо слова «культура» часто говорят «здесь так принято» или «ДНК организации». В организации может быть несколько четко определяемых культур, которые обычно ассоциируются, например, с различными подразделениями, уровнями иерархии или должностями. Если одна культура в принципе не приемлет рисков, а другая охотно идет на риск (такое часто наблюдается при взаимодействии подразделений, отвечающих за производственную безопасность и за внедрение инновационных технологий), появляются трения. Вот почему руководство должно последовательно прививать культуру организации во всех ее подразделениях.

В основе культуры организации лежит доверие. В ходе пятого вебинара цикла «Обеспечение промышленной безопасности и охраны труда в период ограничительных мер, связанных с распространением COVID-19, и на дальнейшую перспективу»[12] представитель международной организации World Ethical Data Foundation Джон Маршалл отметил, что доверие существует всегда, но бывают случаи, когда люди не заслуживают доверия или злоупотребляют им, а ведь вновь завоевать утраченное доверие очень и очень сложно. Там, где существует доверие, оно оказывается очень эффективным и создает культуру, в которой люди раскрывают весь свой потенциал и стараются работать как можно лучше. Это дает существенные преимущества всей организации, улучшая следующие ее аспекты:

- ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ
- ОХРАНА ТРУДА И ТЕХНИКА БЕЗОПАСНОСТИ

11) ISO 45001:2018, Приложение A

12) https://www.unido.org/ensuring-industrial-safety-and-security-times-covid-19-and-beyond

- НОРМАТИВНО-ПРАВОВОЕ СООТВЕТСТВИЕ
- КАЧЕСТВО
- ПРОИЗВОДИТЕЛЬНОСТЬ
- УДОВЛЕТВОРЕННОСТЬ РАБОТОЙ И МОРАЛЬНО-ПСИХОЛОГИЧЕСКОЕ СОСТОЯНИЕ
- ПРИЕМ НА РАБОТУ И УДЕРЖАНИЕ ПЕРСОНАЛА
- РЕПУТАЦИЯ
- И, РАЗУМЕЕТСЯ, УСТОЙЧИВОСТЬ ОРГАНИЗАЦИИ К ВНЕШНИМ ВОЗДЕЙСТВИЯМ

Культуру доверия невозможно создать за один день. Это требует времени, старания и постоянных усилий – того, что именуется «культурной зрелостью». Консультант Международного агентства по атомной энергии Кэролайн Пайк в ходе того же вебинара использовала следующую аналогию: чтобы у вас в саду было красиво, нужно хорошо потрудиться, а затем постоянно ухаживать за садом, чтобы он не зарос сорняками. Ключевые аспекты, наличие которых позволит создать позитивную культуру:

ОРИЕНТИРОВАННОЕ НА СОТРУДНИЧЕСТВО, КОММУНИКАТИВНОЕ, ЭМОЦИОНАЛЬНО ГРАМОТНОЕ РУКОВОДСТВО

В сфере промышленной безопасности это включает понятия, близкие культурам «беспристрастности», «восстановления» и «обучения», в которых неисправности возникают не по вине конкретного человека, а являются результатом системных организационных проблем, которые часто называют факторами, влияющими на эффективность (ФВЭ)[13] . Противоположностью этого является культура страха, в которой человек опасается сообщать о вопросах, вызывающих обеспокоенность, так как ожидает за это санкций вплоть до увольнения.

ВИДЕНИЕ И ЦЕННОСТИ

Необходимо четко соотносить видение и ценности организации с ее повседневной деятельностью. Ярким примером тому в сфере промышленной безопасности, охраны труда и техники безопасности является концепция «нулевого травматизма» или «безаварийности». Это может быть убедительным заявлением о намерениях со стороны руководства. Но каким образом транслировать его на уровень персонала и конкретных производственных операций? Какие конкретные изменения необходимо осуществить в повседневной деятельности для повышения уровня безопасности? Часто речь идет скорее о долгосрочных устремлениях, нежели о ряде практических конкретных действий. Но это следует четко проговорить. Иначе, когда повседневные оперативные решения войдут в противоречие со стремлением к «нулевому травматизму», правдивость сообщения будет поставлена под сомнение, что приведет к кризису доверия. Именно тогда возникает расхождение между видением и реальностью, которое постепенно снижает уровень доверия и ведет к падению мотивации и появлению чувства обиды.

ШИРОКОЕ ОБСУЖДЕНИЕ И ВСЕОБЩЕЕ УЧАСТИЕ

Достоверно известно, что в организациях, которые привлекают рабочий персонал к решению вопросов охраны труда и техники безопасности на рабочих местах, показатели в сфере охраны труда и техники безопасности серьезно улучшаются. Это происходит потому, что рабочие часто располагают большими возможностями для выявления проблем и решений. Когда с ними советуются, рабочие чувствуют, что их уважают и ценят. В свою очередь, это ведет к расширению позитивных (с точки зрения безопасности) поведенческих стратегий. Рабочие во всех сценариях являются ресурсом, потенциал которого нужно использовать, а не проблемой, которую нужно контролировать. Чем лучше система приспособлена к достижению этой цели, тем выше уровень доверия и эффективность самой системы.

13) https://www.hse.gov.uk/humanfactors/topics/pifs.pdf

КОМПЕТЕНТНОСТЬ И РЕСУРСЫ

Это критическая часть культуры организации. Если работники не обладают нужными навыками и умениями, они никогда не добьются оптимальных результатов. Аналогичным образом, если отсутствуют ресурсы, необходимые для выполнения производственных заданий, уровень производительности и безопасности будет предсказуемо заниженным. С точки зрения промышленной безопасности, охраны труда и техники безопасности ключевое значение имеет компетентность в области рисков. Осознают ли работники (на всех уровнях организации) существующие риски и знают ли они, как защитить себя и снизить эти риски? Ведь это является ключевым компонентом зачастую забытой, критически важной части культуры безопасности — «гибкой культуры». Речь идет о предоставлении квалифицированным и знающим работникам полномочий принимать решения «на переднем крае», чтобы достичь целей в области безопасности, даже если это требует адаптации существующего подхода. Эта способность адаптироваться является точкой пересечения культуры безопасности и устойчивости к внешним воздействиям. Чтобы поставить эту способность на службу организации, необходимо вкладывать силы и средства в работников и руководителей.

Хотя пандемия COVID-19 сопряжена с серьезными вызовами, она также создала беспрецедентную возможность укрепить доверие. До начала пандемии COVID-19 многие организации неохотно соглашались на гибкий график или работу из дома. Хотя в качестве причин приводились веские коммерческие соображения (инфраструктура ИТ, обслуживание клиентов), на самом деле организации просто не доверяли своим сотрудникам. Считалось, что, если человек работает из дома, он работает не эффективно. Это предположение было опровергнуто исследованиями и фактами: производительность во многих организациях только возросла. В то время как гибкость и работа из дома — нереалистичный сценарий для многих должностей (особенно в сфере промышленной безопасности), да и не каждый, кто в принципе может работать из дома, хочет этого, организациям следует пересмотреть свое представление о доверии работникам. Те организации, которые этого не сделают, обречены на резкое ухудшение культуры и устойчивости к внешним воздействиям на фоне массового увольнения наиболее перспективных сотрудников. Чтобы помочь организациям создать верную культуру, BSI разработал Модель приоритезации персонала (Prioritizing People Model©). Это модель описывает, что должны представлять собой передовые методы формирования культуры доверия — той самой, которая создает эффективные условия для самореализации (благополучия) работников и устойчивости организации к внешним воздействиям.

4

Проверки соблюдения требований промышленной безопасности

Пандемия COVID-19 также стала серьезным испытанием для органов, осуществляющих надзор за соблюдением требований промышленной безопасности. Периодичность и порядок проверок заводов и предприятий на предмет соблюдения правил безопасности регламентируется законодательством. Но 2020 год показал, что законодательство должно быть достаточно гибким, поскольку в непредвиденных обстоятельствах требуется ввести особый режим контроля и надзора.

Пандемия COVID-19 также стала серьезным испытанием для органов, осуществляющих надзор за соблюдением требований промышленной безопасности. Периодичность и порядок проверок заводов и предприятий на предмет соблюдения правил безопасности регламентируется законодательством. Но 2020 год показал, что законодательство должно быть достаточно гибким, поскольку в непредвиденных обстоятельствах требуется ввести особый режим контроля и надзора.

С одной стороны, представляется очевидным, что количество проверок следует сократить с целью свести к минимуму личные контакты, но, с другой стороны, нельзя игнорировать проблемы обеспечения безопасности, поскольку они могут повлечь за собой неприятные последствия, например происшествия и аварии.

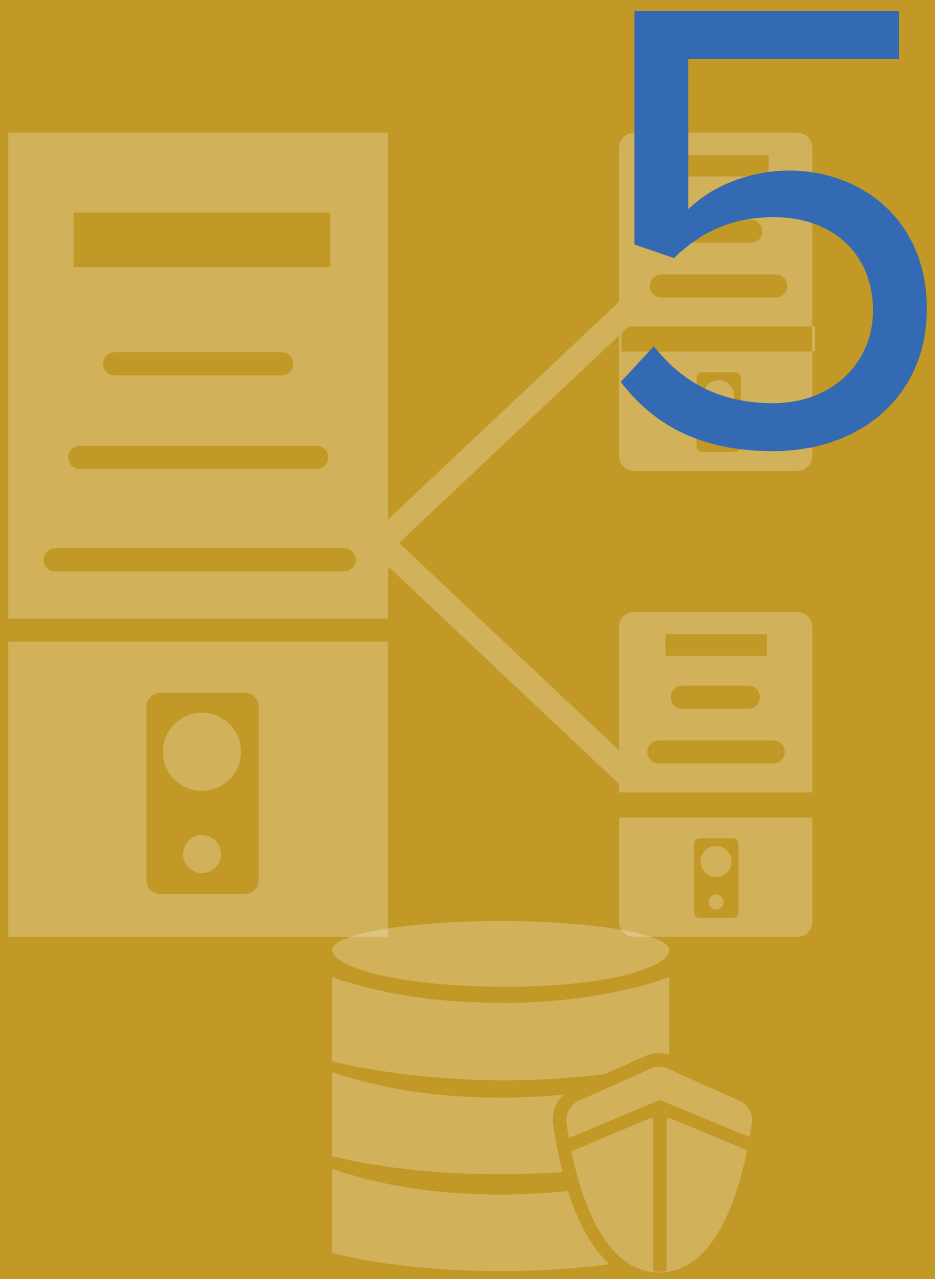
Вот почему в таких условиях критически важно определить потенциально опасные объекты, надзор за которыми государственным органам следует осуществлять на месте с учетом опасностей и рисков, а также санитарно-эпидемиологических ограничений, которые предписывают проверяющим соблюдать социальную дистанцию и носить средства индивидуальной защиты, включая медицинские маски и перчатки.

Проверки объектов с невысокой степенью опасности можно проводить по аудио- и видеосвязи, а также с использованием инструментов удаленного взаимодействия. Для этого следует оборудовать специальный информационный центр, куда будут поступать результаты анализа документации и данные из информационных систем предприятий.

В условиях пандемии COVID-19 органы, осуществляющие надзор за соблюдением требований промышленной безопасности, должны принять специальные меры для обеспечения безопасной работы предприятий и использовать различные методы удаленного взаимодействия, сводя к минимуму количество требуемых документов, а также продлевая срок действия ранее выданных документов на основании результатов предыдущих проверок.

Технологии, повышающие уровень безопасности

Благодаря развитию технологий мы теперь можем постоянно контролировать соблюдение требований промышленной безопасности, охраны труда и техники безопасности. Речь идет главным образом об использовании дистанционных аудитов и проверок. Аудиты в основном заключаются в анализе документов и данных, осмотрах помещений, подтверждении реализации тех или иных мер и беседах с работниками с помощью различных цифровых инструментов.



Технология является важным компонентом безопасности персонала в практике безопасного производства работ во время эпидемии COVID-19: возможность работать из дома или повышать квалификацию онлайн сводит риск заразиться к минимуму, использование систем бесконтактного доступа и эксплуатации снижает риск передачи инфекции, а мобильные приложения позволяют фиксировать ваши перемещения, обеспечивая быстрое отслеживание и контроль. Благодаря развитию технологий, мы также можем постоянно контролировать соблюдение требований промышленной безопасности, охраны труда и техники безопасности. Речь идет главным образом об использовании дистанционных аудитов и проверок.

Дистанционные и иммерсивные аудиты (а также проверки) в целом схожи с аудитом на местах. Разница лишь в том, что аудитор использует инструменты удаленного взаимодействия. Аудиты заключаются в анализе документов и данных, осмотрах помещений, подтверждении реализации тех или иных мер и беседах с работниками и т. п. с помощью различных цифровых инструментов, в том числе:

Технологии, поддерживающие трансляции в реальном времени, например Webex, Zoom, MS Teams, GotoWebinar.

Трансляции в реальном времени плюс мобильные технологии, то есть смартфон или планшет с видеовозможностями (например WhatsApp, WeChat, Skype, Facetime).

Трансляции в реальном времени плюс смартфон, планшет, умные очки и гарнитура для просмотра видео.

Помимо высокой степени уверенности, иммерсивный аудит обладает и другими преимуществами. Он позволяет уменьшить число поездок (что благоприятно сказывается на окружающей среде), проводить более частые и точечные проверки, повысить эффективность оценки при принятии решения о нарушении, а также привлекать специалистов различного профиля. Кроме того, иммерсивные аудиты обеспечивают более высокий уровень вовлечения при аудите или проверке за счет повышенной прозрачности в части несоответствий, передовых методов и наблюдений общего характера.

Проведение дистанционного аудита сопряжено с определенными трудностями. Использование цифровых инструментов «реального времени» не всегда возможно в случае проблем с подключением. В подобных обстоятельствах следует использовать другие методы, например видеосъемку: человек, находящийся на месте, может снять видео конкретного процесса, а затем отправить его по электронной почте (или с помощью другого инструмента совместного использования) для индивидуального просмотра. Иногда использовать цифровые инструменты рискованно (например, во взрывоопасных атмосферах). В подобных средах применение искробезопасной технологии позволяет устранить риски и продолжить иммерсивный аудит. Все стороны, участвующие в аудите, должны обладать компетенциями, необходимыми для использования и проведения иммерсивного аудита, а также учитывать последствия психологической усталости, поскольку дистанционный аудит может вызывать переутомление.

Существует еще одна проблема: некоторые стандарты, органы по аккредитации и органы законодательной власти не успевают за ростом популярности дистанционного аудита. Яркий пример: в секторе автомобилестроения Международная автомобильная целевая группа (IATF) не разрешила дистанционный аудит в рамках своей сертификации системы менеджмента качества и пошла на уступки лишь несколько месяцев спустя, прислушавшись к аргументам представителей отрасли и сертификационных органов. Похожая ситуация возникла в продовольственном секторе — предложение совместить аудиты с проверками качества пищевых продуктов было отклонено. И наоборот, авиационно-космическая отрасль отреагировала быстро: Международная авиакосмическая группа по качеству (IAQG) подготовила четкие указания по проведению дистанционного аудита, обеспечив высокую степень уверенности на весь период пандемии.

Иммерсивные аудиты имеют несомненную ценность, однако, по общему мнению, не могут полностью заменить физические аудиты, особенно в сфере промышленной безопасности, охраны труда и техники безопасности. Поэтому понадобится смешанный подход. Теперь всем заинтересованным лицам необходимо быстро организовать совместное обсуждение и договориться, что будет представлять собой эта смешанная модель. До сих пор мы просто проводили виртуальный аудит в соответствии с принципами физического аудита. Регуляторам, разработчикам стандартов и органам по аккредитации следует начать мыслить по-новому. Если они будут и дальше оценивать новый смешанный подход, опираясь на показатели прежнего подхода, то останутся позади, в то время как промышленность стремится в опережающем темпе извлекать выгоды из цифровизации. И действительно, у этих органов есть отличная возможность более эффективно использовать цифровой след организаций для аудиторской деятельности и контроля за исполнением требований, благодаря

таким инструментам, как непрерывный мониторинг.

Сектор систем удаленного непрерывного мониторинга демонстрирует быстрый рост и обладает огромным потенциалом с точки зрения соответствия требованиям и контроля за их исполнением. Особенно активно осваивают эти системы специалисты по промышленной безопасности. В сфере промышленной безопасности уже используется широкий диапазон эксплуатационных технологий. В настоящее время мы наблюдаем процесс связывания этих технологий с аналитическими и цифровыми инструментами, что позволит создавать модели прогнозирования рисков. То же самое происходит в сфере охраны труда и техники безопасности в строительстве и при использовании технологии информационного моделирования зданий и сооружений (BIM). Возможность прогнозировать еще не случившиеся происшествия, связанные с безопасностью и качеством, — очень убедительный аргумент, особенно в сфере промышленной безопасности, где любое происшествие может иметь трагические и долговременные последствия для людей и окружающей среды. Тем не менее, мы должны проявлять осмотрительность в отношении возможностей, которые открывает перед нами цифровизация и индустрия 4.0. Мы не можем перекладывать ответственность за обеспечение безопасности на технологические решения, особенно с учетом того, что технологии часто дают сбои. Рассмотрим, к примеру, искусственный интеллект. Алгоритмы, лежащие в основе этого мощного инструмента, пишутся людьми, а люди привносят в них осознанные и неосознанные искажения. К тому же существует риск ошибки человека из-за низкого качества управления показателями работы персонала (см. раздел «Культура»). Всё это может увеличить риски, связанные с использованием технологий, тогда как мы ожидаем их уменьшения.

Кроме того, важно не упускать из виду основные проблемы обеспечения безопасности. 4 августа 2020 года Ближний Восток сотряс взрыв, который считается одним из самых мощных в истории человечества неядерных взрывов, вызванных антропогенными причинами. Взорвалась большая партия аммиачной селитры, которая хранилась на складе в порту Бейрута. Погибло 210 человек, разрушен порт и несколько районов города. Расследование еще не завершено, но уже сейчас ясно, что этот высокоопасный химикат в течение нескольких лет хранился с нарушением правил техники безопасности. Взрыву предшествовал пожар, который, возможно, был вызван работами, связанными с нагревом и применением пламени. Хранение химреагентов и работы, связанные с нагревом и применением пламени, относятся к основным проблемам обеспечения безопасности. Мы должны убедиться, что эффективно управляем этими основными угрозами безопасности, чтобы избежать трагических последствий.

И, наконец, индустрия 4.0 привела к появлению новой проблемы обеспечения безопасности, которую стоит отнести к «основным» в рамках наших стратегий управления рисками. Речь идет о кибербезопасности.

Кибербезопасность

6

Управление рисками занимает центральное место в кибербезопасности и промышленной безопасности. Тем не менее, результативное взаимодействие на двух этих направлениях встречается редко. Устранение этих барьеров имеет ключевое значение для обеспечения комплексной безопасности (кибербезопасности и промышленной безопасности).

Как упоминалось выше, вот уже многие годы в сфере промышленной безопасности используют широкий диапазон эксплуатационных технологий — главным образом, для промышленных систем управления. Тем не менее, на фоне системной работы по выявлению, оценке и устранению угроз безопасности зачастую не уделяют должного внимания рискам, связанным с кибербезопасностью этих систем. Это подчеркивает актуальность одного из фундаментальных аспектов культуры, который мы рассматривали ранее: имеется ли в организации достаточно высокий уровень компетентности в области рисков? Это также подчеркивает важность другой составляющей культуры, о которой также упоминалось: речь об умении межфункциональных групп эффективно взаимодействовать друг с другом. Управление рисками занимает центральное место в кибербезопасности и промышленной безопасности. Тем не менее, результативное взаимодействие на двух этих направлениях встречается редко. Устранение этих барьеров имеет ключевое значение для обеспечения комплексной безопасности (кибербезопасности и промышленной безопасности).

Многочисленные барьеры и проблемы на стыке промышленной безопасности и кибербезопасности оказались в центре внимания после недавней кибератаки на станцию водоподготовки во Флориде, когда злоумышленник попытался отравить питьевую воду[14].

НЕ УСТАНАВЛИВАЮТСЯ ИСПРАВЛЕНИЯ И ОБНОВЛЕНИЯ СИСТЕМЫ

Промышленные системы управления используются во многих организациях уже несколько лет. Зачастую эти организации не торопятся обновлять информационные технологии, опасаясь сбоев критических для эксплуатации (а иногда и для безопасности) систем. Вот почему вместо того, чтобы устанавливать обновления, разработанные для повышения уровня кибербезопасности, они в принципе не устанавливают обновления. Именно поэтому взломщик смог проникнуть в компьютерную сеть на станции водоподготовки во Флориде, которая находилась под управлением устаревшей версии Windows 7. Следовательно, своевременно устанавливать обновления — критически важно. Если при установке обновлений действительно возникают проблемы, связанные с эксплуатацией или промышленной безопасностью, специалисты в сфере кибербезопасности / промышленной безопасности вместе с эксплуатационными группами должны предложить эффективные альтернативы, например правильную сегментацию сети и развертывание архитектуры на основе модели «Никому не доверяй».

14) https://us-cert.cisa.gov/ncas/alerts/aa21-042a

ОТСЛЕЖИВАНИЕ И СЕГМЕНТАЦИЯ РЕСУРСОВ

Промышленные системы управления стали чересчур сложными. В результате не всегда есть четкое понимание того, какие ресурсы в действительности существуют, и (с точки зрения кибербезопасности) связаны ли они друг с другом или с сетью Интернет и, если связаны, то каким образом. Подобные системы являются гораздо более легким объектом атаки злоумышленников: поскольку они не сегментированы (не отделены друг от друга / общей ИТ-системы), злоумышленник может перемещаться по всей системе в поисках более привлекательной цели. Компьютер, установленный на станции водоподготовки во Флориде, судя по всему, был подключен к сети Интернет напрямую, минуя брандмауэр. Вот почему организации должны постоянно вести реестр ресурсов и понимать, каким образом они выходят в Интернет и как они связаны с другими элементами инфраструктуры ИТ. Эти (и многие другие) передовые методы описаны в международном стандарте менеджмента информационной безопасности ISO 27001.

КОМПЕТЕНТНОСТЬ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Создается впечатление, что на всех компьютерах станции водоподготовки во Флориде и для удаленного доступа к приложению, обеспечивающему совместный доступ к рабочему столу, использовался один и тот же пароль. Подобрав этот пароль, злоумышленник получил доступ в систему. Хотя существует множество элементов управления, которые можно и нужно использовать (например, многоэтапная аутентификация и генераторы случайных паролей), проникновение в системы чаще всего осуществляется с помощью методов социальной инженерии (фишинг и т. п.). Поэтому для сотрудников на всех уровнях организации следует провести обучение, после которого они смогут выявлять риски, связанные с кибербезопасностью, и будут знать, какие действия следует предпринять для устранения или снижения такого риска.

ТРЕТЬИ ЛИЦА

Несмотря на то, что эта проблема не была выявлена по результатам происшествия на станции водоподготовки во Флориде, наличие третьих лиц является еще одним существенным риском. Третьи лица (подрядчики, поставщики, заказчики) могут иметь доступ к любому количеству систем. Производители комплектного оборудования (OEM-компании) часто настаивают на том, что им необходимо самим устанавливать обновления и исправления в свое оборудование, и оставляют точки доступа, чтобы упростить процесс установки. Эти точки доступа могут быть использованы злоумышленниками. В такой ситуации главное — применять эффективные средства контроля доступа, причем для разных систем разные.

ИЗМЕНЕНИЯ В ЗАКОНОДАТЕЛЬСТВЕ

Во многих юрисдикциях были приняты требования в сфере кибербезопасности: начиная от директивы NIS (директивы по безопасности сетевых и информационных систем) Агентства Европейского союза по кибербезопасности (ENISA) и заканчивая требованиями в рамках CMMC (сертификации модели зрелости кибербезопасности) Министерства обороны США и особыми законодательными требованиями штата Калифорния.

Например, требования директивы NIS распространяются на критически важные отрасли (энергетика, транспорт, водные ресурсы, здравоохранение, цифровая инфраструктура и финансовый сектор) и предусматривают разработку правительствами стран-членов национальных стратегий безопасности сетевых и информационных систем. Они должны охватывать следующий круг вопросов: методы сотрудничества между государственным сектором и частным сектором, повышение осведомленности, обучение и образование, программы НИОКР по стратегии NIS, а также программы оценки рисков.

Закон «О кибербезопасности» Европейского Союза содержит исчерпывающее описание правил сертификации в области кибербезопасности для продуктов, процессов и услуг. Кроме того, закон «О кибербезопасности» определяет новый постоянный круг полномочий агентства ENISA, а также предусматривает выделение агентству дополнительных ресурсов для достижения поставленных перед ним целей.

Все указанные выше новые требования затрагивают практически каждую организацию и прежде всего — производственные компании с широким спектром промышленных систем управления, которые во многих случаях по-прежнему используют информационные технологии 1980-х годов, что серьезно затрудняет (а иногда и исключает) их обновление в соответствии с самыми современными требованиями к информационной безопасности. Длительный жизненный цикл производств и тенденция «не чинить, пока не сломается» с течением времени ведут к увеличению риска, поскольку известные уязвимости со временем будут привлекать внимание всё большего числа злоумышленников. В конце концов, с точки зрения эксплуатации, если система управления исправна, зачем заменять вполне исправно работающее оборудование на новое? Безусловно, следует взять на вооружение упреждающий подход, согласно которому организации обязаны обеспечить кибербезопасность на всех направлениях своей деятельности (насколько это практически осуществимо). Это позволит организациям заранее оценить свои киберриски и внедрить эффективные механизмы управления, которые соответствуют их потребностям и обстоятельствам. Подобный подход на основе эффективности позволит найди золотую середину между общественной безопасностью, подотчетностью и результативностью.

Многие современные организации зависят от разветвленных цепочек поставок и цифрового соединения с поставщиками — в диапазоне от совместного использования проектных файлов до обработки заказов и от управления запасами до финансовых систем. При этом зачастую организации не понимают важность безопасности цифровой цепочки поставок или, как минимум, не уделяют этому вопросу должного внимания. В то время как многие организации осознают влияние поставщиков на качество своей продукции, они часто не придают значения влиянию цепочки поставок как на их собственную информационную безопасность, так и на непрерывность бизнеса и его устойчивость к внешним воздействиям.

Заключение и итоги

В этом справочнике мы постарались показать, что в некоторых случаях у сложных проблем бывают простые решения. Тем не менее, организации должны вовремя начать и последовательно осуществлять эти простые шаги, которые, в конечном счете, сделают наш мир и условия труда более безопасными. Это позволит не только улучшить качество жизни людей, но и сведет к минимуму затраты, связанные с ликвидацией последствий серьезных происшествий. Поиск легких путей в сфере безопасности может причинить серьезный вред и, в ряде случаев, привести к серьезным затратам, которые нередко в конечном счете ложатся на органы государственной власти.

Вот почему следует обратить внимание на этот справочник, который дает общее представление о том, в какой точке следует начинать эти простые шаги и каким образом обеспечить безопасные и благоприятные условия труда в разных отраслях. Следует рассмотреть различные модели и выбрать ту, которая будет наиболее эффективна в сложившихся обстоятельствах, придавая особое значение упреждающему управлению безопасностью и надлежащим мерам контроля.

В ходе осуществления проекта ЮНИДО «Обеспечение промышленной безопасности и охраны труда» группа экспертов и сеть, созданная для достижения цели проекта, состоящей в повышении уровня безопасности и охраны труда во всем мире, смогли привлечь пристальное внимание ко всему спектру вопросов. Был сделан акцент на том, что безопасность — это не сфера ответственности исключительно регуляторов, исключительно компании или исключительно работника. Важно осознать динамическую природу этих отношений и извлечь необходимые уроки для всех заинтересованных лиц. Для этого в мае 2019 года была проведена представительная Конференция по обеспечению промышленной безопасности и охраны труда, в которой приняли участие более 80 ведущих экспертов в сфере безопасности, представители правительства и службы государственного надзора в сфере техники безопасности, а также поставщики технологий обеспечения безопасности.

В качестве следующего шага и на основе многочисленных положительных отзывов по итогам конференции, а также в ответ на пандемию COVID-19 мы оперативно организовали цикл вебинаров, чтобы облегчить поиск решений в кризис, который на тот момент не ослабевал, а во многих странах и сейчас продолжает набирать обороты. Пандемия COVID-19 стала серьезным вызовом как для передовых, так и для проблемных систем безопасности. Это еще раз подчеркивает важность обеспечения долгосрочного планирования, когда речь заходит о вопросах безопасности.

Используя накопленный опыт, мы разработали передовые методы в области безопасности и знаем, как избегать опасных происшествий. Тем не менее, они по-прежнему случаются в разных странах мира. Локдауны и пандемия в некоторых случаях привели к перекрытию потока критической информации, но при этом предоставили новые возможности (включая дистанционные проверки и удаленный мониторинг), которые могут увеличить объем и повысить качество информации, поступающей в адрес регуляторов и органов, осуществляющих надзор за соблюдением требований безопасности. Есть вероятность, что это позволит повысить уровень безопасности восстанавливающихся отраслей. Более того, стремительный прогресс в сфере мониторинга, проверок и оценки может дать новый импульс процессу оптимизации информации как в промышленности, так и на уровне регуляторов. Был выявлен значительный потенциал для сотрудничества и есть все основания рассчитывать, что он будет реализован в полной мере.

В ближайшем будущем рассматриваемая тема и направления сотрудничества, сформировавшиеся в ходе этого проекта, останутся в повестке международных форумов и других форматов диалога. Мы должны приложить все усилия, чтобы повысить уровень безопасности во всем мире, сделать экономики более устойчивыми к внешним воздействиям и функционирующими в интересах всего населения, а также воплотить в жизнь видение всеобщего устойчивого промышленного развития.

Дополнительные материалы

[1] Agnew, J., 2013. Building the Foundation for a Sustainable Safety Culture.
Размещено по адресу: https://www.ehstoday.com/ sustainable-safety-culture.

[2] Bauer, A., Wollherr, D. and Buss, M., 2008. Human-Robot Collaboration: A Survey.
International Journal of Humanoid Robotics, 5, 47–66. 10.1142/ S0219843608001303

[3] Bridgestone, n.d. Safety, Industrial Hygiene.
Размещено по адресу: https://www.bridgestone.com/responsibilities/safety_health/index.html.

[4] British Safety Council, 2017. Five Star Occupational Health and Safety Audit.
Размещено по адресу: https://www.britsafe.org/media/3388/ma176-fsa-hs-spec-v6–2507.pdf

[5] Estimates of the Cancer Burden in Europe from Radioactive Fallout from the Chernobyl Accident. International Journal of Cancer. Cardis et al. (2006).

[6] Frick, K. and Zwetsloot, G.I.J.M., 2007. From Safety Management to Corporate Citizenship: An Overview of Approaches to Health Management. In: U. Johansson, G. Ahonen & R. Roslander (editors), Work Health and Management Control, Thomson Fakta, Stockholm,pp. 99–134.

[7] Haimes, Y.Y., 2009. Risk Modeling, Assessment, and Management.
New York, NY: John Wiley & Sons, pp. 154–196.

[8] HSE (Health and Safety Executive), 2000. Safety Culture Maturity Model: Offshore Technology Report 2000/049.
Keil Centre for the Health and Safety Executive.

[9] 2005. A Review of Safety Culture and Safety Climate Literature for the Development of the Safety Culture Inspection Toolkit. Research Report 367. Crown Publishers.
Размещено по адресу: http://www.hse.gov. uk/research/rrpdf/rr367.pdf.

[10] HSL (Health and Safety Laboratory), 2002. Safety Culture: A Review of the Literature. Crown Publishers.
Размещено по адресу: http://www.hse.gov.uk/research/hsl_pdf/2002/ hsl02-25.pdf

[11] ICSI (Institut pour une Culture de Securite Industrielle) Safety Culture Working Group, 2017. Safety Culture: From Understanding to Action. Issue 2018-01 of the Cahiers de la Securite Industrielle collection. Toulouse, France: ICSI.
https://www.icsi-eu.org/documents/88/csi_1801-_ safety_culture_from_understanding_to_action.pdf

[12] ISO (International Organization for Standardization), n.d. ISO 45001 Occupational Health and Safety. Geneva: ISO.
Размещено по адресу: https://www.iso.org/iso-45001 -occupational-health-and-safety.html

[13] Building a Safety Culture: Improving Safety and Health Management in the Construction Industry SmartMarket Report. Centre for Construction Research & Training. Dodge Data & Analytics. DuPont, The DuPont™ Bradley Curve™.
Размещено по адресу: https://www.consultdss.com/bradley-curve/Jones et al. 2016.

[14] OSG (Occupational Safety Group), n.d. Six Tips to Help you Build a Positive Safety Culture.
Размещено по адресу: https://osg.ca/six-tips-to-help-you-build-a-positive -safety-culture-in-your-workplace/

[15] UN (United Nations), n.d. Global Indicator Framework for the Sustainable Development Goals and Targets of the 2030 Agenda for Sustainable Development. New York: United Nations.
Размещено по адресу: https://unstats.un.org/sdgs/indicators/Global%20Indicator%20Framework%20after%20 2019%20refinement_Eng.pdf

[16] University of Cambridge. 2019a. Managing Cyber Risk in the Fourth Industrial Revolution: Characterizing Cyber Threats, Vulnerabilities and Potential Losses.

[17] 2019b. OK Computer? The Safety and Security Dimension of Industry 4.0.

[18] 2019c. Safety Assurance of Autonomy to Support the Fourth Industrial Revolution.

Список использованных источников

[1] Hämäläinen, P., Takala, J. and Boon Kiat, T., 2017. Global Estimates of Occupational Accidents and Work-related Illnesses 2017. XXI World Congress on Safety and Health at Work. Singapore: Workplace Safety and Health Institute.
Размещено по адресу: http://www.icohweb. org/site/images/news/pdf/Report%20Global%20 Estimates%20of%20 Occupational%20Accidents%20 and%20Work-related%20Illnesses%202017%20rev1.pdf.

[2] ILO (International Labour Organization), 2019. Safety and Health at the Heart of the Future of Work: Building on 100 Years of Experience. Geneva: ILO, p. 3.
Размещено по адресу: https://www.ilo.org/wcmsp5/ groups/public/---dgreports/---

[3] United Nations Industrial Development Organization, 2019. International Conference on Ensuring Industrial Safety: The Role of Government, Regulations, Standards and New Technologies. Vienna.

www.unido.org

Этот проект финансируется
Российской Федерацией

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
ПО ПРОМЫШЛЕННОМУ РАЗВИТИЮ

Международный центр в Вене · P.O. Box 300 · 1400 Vienna · Austria (Австрия)
Телефон: (+43-1) 26026-0 · unido@unido.org
www.unido.org