

Аннотация статьи: «Методические подходы к оценке влияния компьютерных инцидентов на возникновение и развитие технологических инцидентов и (или) аварий, приводящих к пожарам и взрывам на опасных производственных объектах в целях обеспечения пожаровзрывобезопасности технологических процессов»
08.06.2026 г.

С.Д. Кисляков, В.П. Космачев, С.Б. Обломский (ООО «НТЦ «ТБ»)

Использование современных автоматизированных систем управления технологическим процессом, а также активное их совершенствование позволяют эффективно осуществлять управление и контроль в производственной сфере, но при этом вызывают повышенные требования к обеспечению их безопасности от несанкционированного доступа.

В связи с широким распространением информационных технологий, ростом сложности и, следовательно, уязвимости информационной составляющей критической инфраструктуры возрастают информационные (компьютерные) риски для критической информационной инфраструктуры.

Анализ возможных угроз безопасности информации, приводящих к сбоям в работе критически важных объектов, позволяет вывод о том, что наиболее опасными событиями, связанными с нарушениями в работе АСУ ТП является разгерметизация технологического оборудования, вызванная механическим (влияние повышенного или пониженного давления, динамических нагрузок и прочее), температурным (влияние повышенных или пониженных температур) и агрессивным химическим (влияние кислородной, сероводородной, электрохимической и биохимической коррозии) воздействиями.

В настоящее время представляется актуальным разработка методики оценки влияния компьютерных инцидентов на возможность возникновения технологических инцидентов и аварий, приводящих к пожарам и взрывам на опасных производственных объектах в целях обеспечения пожаровзрывобезопасности технологических процессов на стадии эксплуатации. Важнейшим в этом контексте видится именно аспект защиты критически важных объектов и инфраструктур, так как последствия компьютерных атак на них могут быть катастрофическими.

В настоящей статье представлен анализ возможных угроз для критической информационной инфраструктуры, рассмотрены и проанализированы основные (ключевые) нормативно-правовые акты, устанавливающие требования безопасности на объектах топливно-энергетического, регулирование в области защиты объектов критической информационной инфраструктуры от актов незаконного вмешательства.

В статье предлагаются методические подходы к идентификации влияния компьютерных инцидентов на возникновение технологических инцидентов или аварий на опасных производственных объектах для определения степени их защищённости. Методические подходы позволяют ответить на следующие вопросы:

- как влияет компьютерный инцидент на технологический процесс и на безопасность критической информационной инфраструктуры в целом;
- к чему может привести воздействие компьютерного инцидента, какие сценарии развития последствий компьютерного инцидента;
- могут ли существующие (проектные) барьеры безопасности организационного и технического характера обеспечить устойчивое функционирование объекта критической информационной инфраструктуры и предотвратить последствия компьютерного

инцидента.

Методология идентификации влияния компьютерных инцидентов на возникновение технологических инцидентов или аварий состоит из экспертного обсуждения командой компетентных специалистов методом мозгового штурма. В статье подробно описаны этапы поведения процедуры.

Предлагаемые методические подходы по идентификации влияния компьютерных инцидентов на возникновение технологических инцидентов или аварий на опасных производственных объектах позволяют:

- определить влияние компьютерных инцидентов на технологический процесс, функционирование РСУ и ПАЗ;
- разработать сценарии развития отклонений параметров технологического процесса связанных с воздействием компьютерных инцидентов, с учетом анализа возможности его влияния на выполнение идентифицированных функций безопасности, систем противопожарной защиты;
- оценить риски гибели людей в результате воздействия опасных факторов пожара.

Результаты анализа влияния компьютерных инцидентов на безаварийное функционирование опасного производственного объекта позволяют оценить достаточность или недостаточность предусмотренных мер защиты (в том числе систем противопожарной защиты), оценить степень защищенности опасных производственных объектов, выработать рекомендации по дополнительным мерам защиты в случае их необходимости.