УДК 519.8:614.838+510.6:62-7:007.51:004.056.53
DOI: 10.32686/1812-5220-2018-15-80-91

# Мониторинг безопасности информатизированных котельных с сетевым доступом и оценкой риска на логико-вероятностной модели

ISSN 1812-5220


**М. В. Шептунов,**
ФГБОУ ВО «Российский государственный гуманитарный университет» (РГГУ), ФГБОУ ВО «Московский государственный лингвистический университет» (МГЛУ)

**Аннотация**

Рассматривается одна из существующих технологий — многосменного мониторинга безопасности, подразумевающая отслеживание целостности информационной системы (ИС) периодически сменяющими друг друга операторами в интервал между диагностиками ими системы — применительно к информатизированным котельным с сетевым доступом. При этом ИС котельной считается защищенной от опасных программно-технических воздействий через компьютерную сеть, только если к началу заданного периода времени целостность системы обеспечена и в течение всего этого задаваемого периода источники опасности не проникают в систему (с вычисляемой вероятностью). Здесь оператор котельной фигурирует в качестве оконечного звена ряда контролируемых, в т.ч. программного уровня, преград для (внешнего) сетевого злоумышленника. Для информатизированных котельных, в зависимости от соотношений для длительности работы оператора в течение каждой смены, задаваемого периода безопасного функционирования и периода между диагностиками, рассматриваются три варианта, характерные при указанной технологии. Обсуждаются возможности применения последней в ракурсе оценки риска чрезвычайных ситуаций (ЧС) в пределах ранее разработанной автором логико-вероятностной модели для информатизированных котельных.

**Ключевые слова:** несанкционированный доступ (НСД), безотказность, риск, компьютерная система обнаружения вторжений.

# Security monitoring of computerized boiler rooms with network access and risk assessment on a logical-probabilistic model

**M. V. Sheptunov,**
Federal State Budgetary Educational Institution of Higher Education (FSBEI HE) "Russian State University for Humanities" (RSUH), FSBEI HE "Moscow State Linguistic University" (MSLU)

**Annotation**
We consider one of the existing technologies, scilicet of the multi-shift safety monitoring, which implies tracking of the integrity of the information system (IS) by periodically replacing each other operators in the interval between diagnostics of the system, in relation to computerized boiler-rooms with network access. Herein the IS of the boiler-house is taken into account as protected from dangerous software-engineering influences through the computer network only if to the beginning of the specified period of time the integrity of the system is ensured and throughout this set period the sources of danger do not penetrate the system (with a calculated probability). Here the operator of the boiler-room figures as an eventual link of the series of the controlled, including the program level, barriers for (external) network malefactor. For computerized boiler-houses, depending on the ratios for the duration of the operator's work during each shift, the specified period of safe operation and the period between diagnostics, three variants are considered that are typical for this technology. The possibilities of applying the latter in the foreshortening of risk assessment of emergency situations (ES) within the previously developed by the author logical-probabilistic model for computerized boiler-houses are discussed.

**Keywords:** unauthorized access (uaA), reliability, risk, computer intrusion detection system.

## Содержание



## Введение

В настоящее время существенную роль в обеспечении безопасности жизнедеятельности страны, различных объектов экономики Российской Федерации играют современные методы мониторинга опасных явлений, представляя собой основу анализа риска в соответствующих сферах человеческой деятельности. Одной из таких наиболее важных сфер является бесперебойное теплоснабжение, осуществляемое на сегодняшний день как информатизируемыми,

так и уже информатизированными котельными с сетевым доступом. И соответственно, не менее актуальны методы и технологии мониторинга безопасности как приоритетной составляющей оценки риска чрезвычайных ситуаций (ЧС) современных котельных, являющихся одновременно и объектами экономики, и объектами информатизации.

Указанная сфера регулируется как Федеральным законодательством (главным образом ФЗ [1]), так и ГОСТами международного уровня (например, [2]), а также другими нормативными документами.

Среди ключевых звеньев практически любой современной котельной принципиально выделить в т.ч. автоматизированное рабочее место (АРМ) оператора. Учитывая, что АРМ чаще всего создается на базе подключаемых к локальным и глобальной сетям ПЭВМ, воплощая наиболее простой вариант автоматизации рабочих мест котельных, приобретают важность и аспекты защиты не только от физического проникновения на рассматриваемый информатизируемый объект, но и от удаленного сетевого вторжения в ракурсе возможного влияния на технологические процессы в котельных.

Актуальные в ракурсе информационно-телекоммуникационных технологий вопросы рисков использования киберпространства, включая АСУ технологическими процессами, рассматривались в т.ч. и на страницах журнала «Проблемы анализа риска» [7, 8 и др.]. В ряде определенных случаев (что ясно в т.ч. из [8]) ущерб, причиненный одному или нескольким ресурсам (информация на носителях и информация, циркулирующая по внутренним каналам компании и проч.), произошедший вследствие аварии либо в результате злоумышленных или неумышленных действий персонала или иных лиц, может оказаться фатальным для жизнедеятельности предприятия и даже привести к его ликвидации или банкротству, ибо котельные — это и объекты экономики.

На сегодняшний день применение именно интегрированных систем безопасности (ИСБ) предприятия для котельных, защищаемых как от физического НСД, так и сетевого несанкционированного доступа, позволяет не только решать возникающие задачи обеспечения безопасности в комплексе, но и повысить эффективность работы отдельных подсистем и составляющих системы.

При этом следует упомянуть в ракурсе актуальности применения систем обнаружения вторжений (СОВ) для информатизированных котельных, что, как известно, эти системы имеют в своем составе среди других модулей также модуль реакции. За счет последнего СОВ способна как послать соответствующее оповещение на консоль администратора и/или выдать звуковой сигнал, при этом записав информацию об атаке (время, IP-адрес нарушителя, IP-адрес/порт цели атаки и т.п.), занеся событие в системный журнал, так и оборвать сетевое соединение. «Последнее слово» здесь тем не менее за человеком-оператором, являющимся одновременно лицом, принимающим решение (ЛПР) в рамках своей компетенции, и «динамичным» («неявно присутствующим») оконечным звеном именно контролируемой защиты системы. Но СОВ может (при ее корректной настройке и наличии, взяв на себя на определенное время часть функций человека-оператора) и запустить определенную программу — соответственно не исключая, при необходимости — что весьма важно для современной котельной, программу(ы) восстановления целостности системы и/или целостности информации, и переконфигурировать межсетевой экран после блокировки IP-адреса, с которого была осуществлена атака. Существенно (и это не противоречит сформированному в статье [8] сценарию опасного состояния системы), что СОВ может быть помещена вне области, защищаемой межсетевым экраном (выступая в роли отдельной подсистемы), когда атаки фиксируются на СОВ, но не проходят через межсетевой экран [3 и др.]. Естественно при логических построениях предполагать, что именно человек-оператор в итоге производит при такой надобности перенастройку и СОВ как одной из подсистем, и ИСБ в целом.

Сегодня немалые усилия прилагаются к обеспечению защищенности от различного рода опасных воздействий и явлений, способных разрушить целостность системы, включая целостность хранимой на жестком диске компьютера и/или циркулирующей по внутренней сети информации.

Не являются исключением и компьютеризированные системы управления процессом функционирования котельных.

При этом под ***целостностью системы*** понимается такое ее состояние, когда обеспечивается достижение целей системы с требуемым качеством.

Соответственно, под ***целостностью информации*** следует понимать такое ее состояние, при котором обеспечивается функционирование информационной системы (ИС) согласно целевому назначению с требуемым качеством.

При технологии многосменного мониторинга безопасности ИС подразумевается, что целостность системы в период между диагностиками отслеживают сменяющие друг друга операторы. Информационная система полагается защищенной от опасных программно-технических воздействий в течение задаваемого периода времени $T_{зад.}$, если к началу этого периода целостность системы обеспечена и в течение него источники опасности не проникают в систему.

При обнаружении проникновения источника опасности предполагается, что человек-оператор ликвидирует таковой, восстанавливая целостность системы. Проникновение источника опасности в систему (ЭВМ) возможно (в разрезе рассматриваемого в нашем случае преодоления защитной (сетевой) «суммарной» именно контролируемой компьютерной преграды) только в случае ошибки (2-го рода) оператора. Безошибочные же действия оператора предусматривают нейтрализацию источника опасности при попытке его внедриться в систему (при полагаемом ничтожно малом времени нейтрализации). Проверка целостности системы, осуществляемая лишь при проведении диагностики, при (каждой) смене операторов в общем случае не делается. Т. е. проникший в одну из смен источник опасности способен активизироваться в последующие смены вплоть до очередной диагностики. Это усложняющее обстоятельство свидетельствует в пользу выбора в качестве основного интегрального показателя для технологии многосменного мониторинга безопасности системы именно вероятности $P_{прон.(j)}$ отсутствия проникновения источника опасности в систему в течение задаваемого периода $T_{зад.(j)}$ непрерывного безопасного функционирования системы.

Соответственно, упомянутая вероятность $P_{прон.(j)}$ обычно является (в задачах анализа, оценки риска) подлежащим оценке показателем, а задаваемый период $T_{зад.(j)}$ относится к требованиям заказчика и способен служить отправной точкой еще при проектировании и/или формировании ИСБ.

Среди исходных данных отводится место следующим величинам: $j$ — условный номер варианта угроз опасных воздействий и способа защиты; (на практике не всегда точно известная) $\sigma_j$ — частота воздействия на систему, осуществляемого с целью внедрения источника опасности; $T_{меж.j}$ — время между окончанием предыдущей диагностики и началом очередной диагностики целостности системы; $T_{диаг.j}$ — длительность диагностики, включая восстановление целостности системы; $T_{нар.j}$ — среднее время наработки оператора на ошибку 2-го рода (момент $\tau$, с которого отсчитывается оставшееся время до завершения периода $T_{зад.(j)}$); $k_j$ — количество смен операторов между соседними диагностиками (между моментами начала соседних диагностик).

Т. е. для трех возможных вариантов технологии многосменного мониторинга безопасности предполагается проведение через определенные промежутки времени регламентной диагностики, системного контроля целостности ИСБ.

*Целью* данной *работы* является выяснение применимости существующей технологии многосменного мониторинга безопасности в качестве составляющей анализа и оценки по логико-вероятностной модели риска ЧС информатизированных котельных с сетевым доступом.

*Научно-практические задачи работы:*

- выявление наиболее целесообразного (из 3 рассматриваемых) варианта технологии многосменного мониторинга безопасности для задаваемых конкретных ключевых параметров при данной технологии;
- способствование анализу и оценке риска чрезвычайных ситуаций (ЧС) информатизированных котельных с сетевым доступом по построенной автором ранее логико-вероятностной модели.

Естественно исходить из того, что нарушитель нормального режима функционирования котельной может быть как обыкновенным хулиганом, так и специально подготовленным профессионалом.

## 1. Рассматриваемые в разрезе многосменного мониторинга безопасности котельных инициирующие события и условия сценария опасного состояния

В статье [8] для сформированного в ней и приведенного на рис. 1 сценария опасного состояния (СОС) на основе полученной путем соответствующих логических построений формулы:

$$f(z_1,...,z_{32}) = \Big\{[z_6(z'_1 z'_2 z'_3 z'_4 z'_5)']' \cdot [z_{24}(z'_{25} z'_{26})']' \times$$
$$\times [z_{22} z_{23} (z'_{18} z'_{19} z'_{20} z'_{21})']' \cdot \{z_{10} z_{11} [z'_9 (z_7 z_8)']']'\}' \cdot (z_{12} z_{13})' \times$$
$$\times (z_{14} z_{15})' \cdot (z_{16} z_{17})' \cdot (z_{27} z_{28})' \cdot (z_{29} z_{30})' \cdot (z_{31} z_{32})'\Big\}' \quad (1)$$

была получена пригодная для расчетов риска ЧС в информатизированной котельной вероятностная функция опасного состояния (ФОС) системы в виде:

$$P\{f(z_1,...,z_{32}) = 1\} = O_c = 1 - \Big\{[1 - O_6 (1 - Б_1 Б_2 Б_3 Б_4 Б_5)] \times$$
$$\times [1 - O_{24} (1 - Б_{25} Б_{26})] \cdot [1 - O_{22} O_{23} (1 - Б_{18} Б_{19} Б_{20} Б_{21})] \times$$
$$\times \{1 - O_{10} O_{11} (1 - [Б_9 (1 - O_7 O_8)])\} \cdot (1 - O_{12} O_{13}) \times$$
$$\times (1 - O_{14} O_{15}) \cdot (1 - O_{16} O_{17}) \cdot (1 - O_{27} O_{28}) \cdot (1 - O_{29} O_{30}) \times$$
$$\times (1 - O_{31} O_{32})\Big\}, \quad (2)$$

где смысл каждого из обозначений нумерованных переменных соответствует указанному на рис. 1 для инициирующих событий и условий (ИС, ИУ) сценарию опасного состояния системы — с учетом нумерации ИС и ИУ.

Естественно, что для как такового расчета риска $O_c$ рассматриваемой чрезвычайной ситуации нам нужны вероятности каждого из ИС и ИУ, входящих в формулу (2). Для их использования могли бы помочь статистические данные (разумеется, при наличии таковых). Нетривиальной и важной задачей представляется определение соответствующих вероятностей опасности для составляющих $O_{27}$, $O_{28}$ вышеуказанной формулы (причем $z_{27}$ — событие обычно сложное, зависящее от относящихся только к нему простых событий с вероятностями $P_{1z_{27}}$, …, $P_{nz_{27}}$, смысл которых ясен — непреодоление (т.е. прочность в вероятностном смысле) каждой соответствующей дублирующей преграды) или же, как вариант, определение (при такой возможности сразу) вероятности в виде выражения $(1 - O_{27}O_{28})$, входящего в формулу (2).

Следует отметить, что в случае некорректной настройки СОВ либо, тем более, ее отсутствия нагрузка по обнаружению и предотвращению сетевых проникновений (даже при наличии (сетевой) «суммарной», т.е. с одним либо более дублирующим звеном, контролируемой компьютерной преграды) в ИСБ в большей степени ложится на человека-оператора.

Рассматриваемая нами в разрезе многосменного мониторинга безопасности котельных часть инициирующих событий и условий сценария опасного состояния, а именно $z_{27}$, $z_{28}$, относится к возможностям удаленных (сетевых) атак на котельную, являющуюся объектом информатизации. «Прочность» человека-оператора как «динамичного» оконечного звена комплексной контролируемой защиты (особенно от сетевых проникновений в систему) «рассеяна» при наличии СОВ (даже при не вполне корректной ее настройке, которую, как предполагаем, осуществляет в конечном счете человек-оператор) между ней и «суммарной» (последовательно преодолеваемой с некоторой вероятностью злоумышленником) именно контролируемой преградой от сетевых проникновений. Предполагается также, что именно человек-оператор производит (при необходимости) перенастройку системы и, как минимум, регулярно отслеживает файл журнала аудита событий в системе, а как максимум — будучи лицом, принимающим решение (ЛПР — на своем уровне) — вмешивается в ее функционирование в основном при сигналах от нее и/или оперативно нейтрализует электронную деятельность злоумышленника, обнаруженную благодаря активности СОВ и/или межсетевого экрана либо иного звена защиты (при наличии такового) или же благодаря собственным активности и корректным действиям (включая, при необходимости, восстановление целостности всей системы).

Отметим, что в сформированном ранее в статье [8] сценарии опасного состояния системы, а именно упомянутой чрезвычайной ситуации в котельной, предполагается независимость всех фигурирующих в нем инициирующих событий (ИС) и инициирующих условий (ИУ) попарно и в совокупности (включая сложное событие $z_{27}$, для которого расчет вероятности $O_{27}$ становится еще более трудным при наличии для отдельной преграды (той

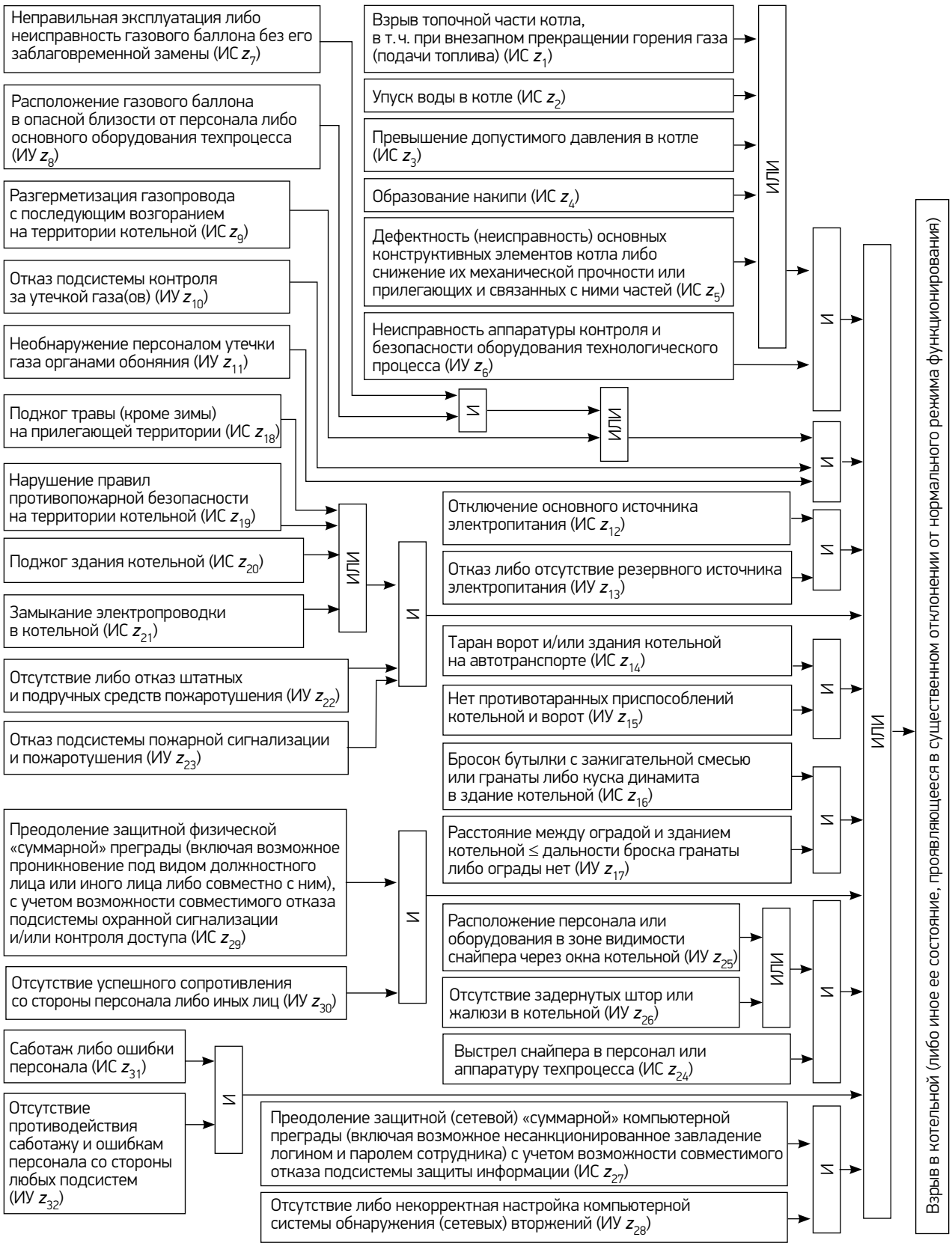


***Рис. 1. Возможный сценарий опасного состояния котельной***

или иной сущности) одной либо более дублирующих ее преград в многозвенной защите).

Важно, что дополнительная (одна либо несколько), т. е. каждая дублирующая преграда должна перекрывать, как минимум, то же количество возможных каналов НСД, что и первая. Отметим и такую отличительную особенность для показанных на рис. 1 ИС $z_{31}$ (саботаж либо ошибки персонала) и для более пристально рассматриваемого в данной статье ИС $z_{27}$ (преодоление защитной (сетевой) «суммарной» компьютерной преграды (включая возможное несанкционированное завладение логином и паролем сотрудника), с учетом возможности совместимого отказа подсистемы защиты информации): событие $z_{31}$ подразумевает ошибки 1-го рода, а событие $z_{27}$ подразумевает ошибки именно 2-го рода.

Далее, обращаясь к рис. 2, пусть нас интересует величина вероятности преодоления (сетевой) «суммарной» преграды нарушителем $P_{нр} = O_{27}$ при наличии в ней всего 2 дублирующих (друг друга) преград; например, одна из них — межсетевой экран, а другая — операционная система компьютера. Как ясно из [5] и [8], $O_{27}$ можно вычислить по формуле

$$P_{нр} = (1 - P_1) \cdot (1 - P_4), \qquad (3)$$

где $P_1$ — прочность (вероятность непреодоления) преграды 1;

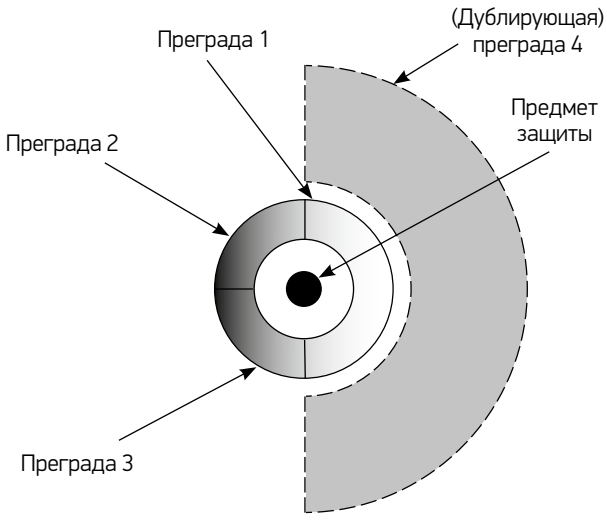


***Рис. 2. Многозвенная защита с отдельными дублируемыми преградами***

$P_4$ — прочность (вероятность непреодоления дублирующей ее) преграды 4.

Тогда вероятность преодоления каждой из них (единственным) нарушителем согласно теории вероятностей как противоположное событие есть соответствующая разность $(1 - P_1), (1 - P_4)$.

Но для расчета нам следует знать обе (для данного случая; а в ряде случаев преград может иметься в системе более 2) прочности дублирующих контролируемых преград $P_1, P_4$.

И, с одной стороны — при невозможности (по какой-либо причине) определить составляющие $P_1$ и/или $P_4$ формулы (3) для расчета $P_{нр} = O_{27}$ (или же для выражения $(1 - O_{27}O_{28})$ только одну $O_{28}$) не представляется на первый взгляд возможным вычислить и значение входящего в (2) выражения $(1 - O_{27}O_{28})$, а соответственно, и вероятность ЧС для информатизированной котельной $O_c$ по формуле (2).

## 2. Выявление наиболее целесообразного варианта многосменного мониторинга безопасности при задаваемых ключевых параметрах данной технологии

Далее нас будет интересовать вопрос о применимости существующей технологии многосменного мониторинга безопасности в качестве составляющей оценки по логико-вероятностной модели риска ЧС информатизированных котельных с сетевым доступом — и в частности — для оценки входящей в формулу (2) величины $(1 - O_{27}O_{28})$ (последнее возможно проделать при неизвестных прочностях $P_i$, образующих $P_{нр} = O_{27}$, и «с другой стороны» — иным рассматриваемым образом с позиций технологии многосменного мониторинга безопасности информатизированных котельных в случае ее применения). И что не менее важно, о наиболее целесообразном варианте технологии многосменного мониторинга безопасности для задаваемых (для трех рассматриваемых вариантов) значений ключевых параметров при данной технологии.

В дополнение к ранее перечисленным (преимущественно во введении) потребующимся нам далее обозначениям укажем $(T_{меж.} + T_{диаг.}) / k$ — длительность работы оператора в течение смены (индекс $j$

для уменьшения громоздкости обозначений опущен сознательно).

Итак, в разрезе известной технологии многосменного мониторинга безопасности возможны три варианта:

- вариант 1 — заданный период безопасного функционирования $T_{зад.}$ меньше длительности работы оператора в течение одной смены, т.е. $(T_{меж.} + T_{диаг.}) / k > T_{зад.}$, где $k$ — количество смен операторов между моментами начала соседних диагностик;
- вариант 2 — заданный период безопасного функционирования $T_{зад.}$ больше или равен длительности работы одного оператора, но меньше периода между диагностиками, т.е. $(T_{меж.} + T_{диаг.}) / k \le T_{зад.} < T_{меж.} + T_{диаг.}$;
- вариант 3: $T_{меж.} + T_{диаг.} < T_{зад.}$, т.е. в течение заданного периода безопасного функционирования $T_{зад.}$ завершится хотя бы одна диагностика.

Для каждого из 3 перечисленных вариантов имеет место свое утверждение относительно вероятности $P_{прон.}(T_{зад.})$ отсутствия источника опасности в системе за заданный период $T_{зад.}$; хотя они известны (преимущественно из [4]), не было обнаружено сведений о применении и/или применимости их в разрезе многосменного мониторинга безопасности именно для информатизированных котельных с сетевым доступом при оценке риска их ЧС по логико-вероятностной модели.

***Утверждение I.*** Для варианта 1 при условии независимости исходных характеристик вероятность $P_{прон.}(T_{зад.})$ *отсутствия* источника опасности в системе за заданный период $T_{зад.}$:

$$P_{прон.(1)}(T_{зад.}) = 1 - \int_0^{T_{зад.}} dA(\tau) \cdot \Omega_{возд.}(T_{зад.} - \tau), \qquad (I)$$

где $\int_0^{T_{зад.}} dA(\tau)$ — вероятность того, что до завершения периода $T_{зад.}$ истечет (среднее) время наработки $T_{нар.(ср.).}$ человека-оператора на ошибку (2-го рода); $\Omega_{возд.}(T_{зад.} - \tau)$ — вероятность того, что в оставшееся время с момента $\tau$ до завершения $T_{зад.}$ осуществится опасное воздействие на систему.

Отметим, что как таковая оценка обеих вышеупомянутых перемножаемых вероятностей для вычисления $P_{прон.(1)}(T_{зад.})$ заслуживает отдельного рассмотрения и не является основной задачей данной статьи, поскольку предполагается, что даже если аналитически ту или иную из этих вероятностей либо обе посчитать крайне сложно (или невозможно), то, по крайней мере, вычислить приближенно и/или с использованием численных методов либо определить на основе экспертных оценок вполне реально.

Пусть для известного (обычно задаваемого заказчиком) $T_{зад.} = 24$ (час.) вычислены (приближенно либо точно) вышеупомянутые: вероятность $\int_0^{T_{зад.}=24} dA(\tau) \approx 0{,}999$ и вероятность $\Omega_{возд.}(T_{зад.} - \tau) \approx 0{,}301$ (для $T_{нар.(ср.).} \approx 4$ (час.)). Вычисленная на основе этих вероятностей по формуле (I) величина интересующей (именно когда более сложно определить все либо какую-либо одну из составляющих вышеупомянутого выражения $(1 - O_{27} \cdot O_{28})$, в котором $O_{27}$ может вычисляться в случае известных всех обычно последовательно преодолеваемых злоумышленником составляющих «суммарной» контролируемой защиты) вероятности $P_{прон.(1)}(T_{зад.} = 24$ (час.)) (для варианта 1) приведена в табл. 4.

Для варианта 2 имеет место известное

***Утверждение II.*** Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия источника опасности в системе за время $T_{зад.}$ равна:

$$P_{прон.(2)}(T_{зад.}) = \frac{L \cdot (T_{меж.} + T_{диаг.}) / k}{T_{зад.}} \times$$
$$\times P^{L}_{прон.(1)}\left(\frac{T_{меж.} + T_{диаг.}}{k}\right) + \frac{T_{ост.(2)}}{T_{зад.}} \times P_{прон.(1)}(T_{ост.(2)}), \quad (II)$$

где $L = [T_{зад.} \cdot k / (T_{меж.} + T_{диаг.})]$ — целая часть;
$T_{ост.(2)} = T_{зад.} - L \cdot (T_{меж.} + T_{диаг.}) / k$ — остаток,
причем для $T_{ост.(2)}$, а не для всего периода $T_{зад.}$ рассчитывается, как для варианта 1, вероятность $P_{прон.(1)}(T_{зад.})$, для которого выполняется условие: $T_{ост.(2)} < (T_{меж.} + T_{диаг.}) / k$.

Пусть, далее, имеются (более-менее реалистичные для информатизированных котельных) исходные данные наряду с $T_{зад.}$, приведенные для варианта 1 и варианта 2 в табл. 1 и табл. 2 — такие, что выполнены соответственно этим вариантам условия (причем $T_{диаг.}$ включает при необходимости время восстановления целостности системы).

*Совокупность используемых в расчете для варианта 1 исходных данных и задаваемого периода $T_{зад.}$* *Таблица 1*

| Время $T_{меж.}$ с момента завершения предыдущей диагностики до начала следующей диагностики (согласно регламенту), час. | Время диагностики $T_{диаг.}$, час. | Количество $k$ смен операторов между соседними диагностиками | Задаваемый период $T_{зад.}$ непрерывного безопасного функционирования системы, час. |
|---|---|---|---|
| 24 | 0,10 | 1 | 24 |

*Совокупность используемых в расчете для варианта 2 исходных данных и задаваемого периода $T_{зад.}$* *Таблица 2*

| Время $T_{меж.}$ с момента завершения предыдущей диагностики до начала следующей диагностики (согласно регламенту), час. | Время диагностики $T_{диаг.}$, час. | Количество $k$ смен операторов между соседними диагностиками | Задаваемый период $T_{зад.}$ непрерывного безопасного функционирования системы, час. |
|---|---|---|---|
| 24 | 0,10 | 2 | 24 |

*Совокупность используемых в расчете для варианта 3 исходных данных и задаваемого периода $T_{зад.}$* *Таблица 3*

| Время $T_{меж.}$ с момента завершения предыдущей диагностики до начала следующей диагностики (согласно регламенту), час. | Время диагностики $T_{диаг.}$, час. | Задаваемый период $T_{зад.}$ непрерывного безопасного функционирования системы, час. |
|---|---|---|
| 23,8 | 0,10 | 24 |

*Промежуточные и итоговые результаты расчетов при рассматриваемых значениях ключевых параметров* *Таблица 4*

| | | | | | | |
|---|---|---|---|---|---|---|
| $P_{прон.(1)}(T_{зад.} = 24$ час.$) \approx$ $\approx 0{,}699$ | $k = 2$ | $L = 1$ | $P_{прон.(1)}\left(\frac{T_{меж.}+T_{диаг.}}{k}\right) \approx$ $\approx 0{,}819$ | $T_{ост.(2)} = 11{,}95$ час. | $P_{прон.(1)}(T_{ост.(2)}) \approx$ $\approx 0{,}820$ | $P_{прон.(2)}(T_{зад.} =$ $= 24$ час.$) \approx 0{,}819$ |
| | $\frac{T_{меж.}+T_{диаг.}}{k} = 12{,}05$ час. | | | | | |
| | $N = 1$ | | $P_{прон.(2)}(T_{меж.} + T_{диаг.}) \approx$ $\approx 0{,}819$ | $T_{ост.(3)} = 0{,}1$ час. | $P_{прон.(1)}(T_{ост.(3)}) \approx$ $\approx 0{,}998$ | $P_{прон.(3)}(T_{зад.} =$ $= 24$ час.$) \approx 0{,}819$ |
| | $T_{меж.} + T_{диаг.} = 23{,}9$ час. | | | | | |

Результаты расчетов вероятности $P_{прон.(2)}(T_{зад.})$ приведены в верхней половине табл. 4. Дадим некоторые пояснения. Для (промежуточного) расчета входящей в (II) вероятности $P_{прон.(1)}\left(\frac{T_{меж.}+T_{диаг.}}{k}\right)$ будем исходить из того естественного предположения, что (при $k = 2$) за меньшее время $\frac{T_{меж.}+T_{диаг.}}{k} =$ $= 12{,}05$ (час.) по сравнению с $T_{зад.} = 24$ (час.), для которого в случае варианта 1 вероятность $\Omega_{возд.}(T_{зад.} - \tau)$ при $\tau \approx 4$ (час.) при полагаемой прямо пропорциональной зависимости от времени, уменьшится практически в $\frac{24-4}{12{,}05} \approx 1{,}66$ (раза), а вероятность $\int_0^{T_{зад.}} dA(\tau)$ (поскольку $\tau \ll T_{зад.}$) практически не изменится. Тогда, уменьшая при вычислениях вероятности $P_{прон.(1)}\left(\frac{T_{меж.}+T_{диаг.}}{k} = 12{,}05 \text{ (час.)}\right)$ по формуле (I) величину уже ранее использовавшейся вероятности 0,301 в $\approx 1{,}66$ раза, получим значение

$P_{прон.(1)}\left(\frac{T_{меж.}+T_{диаг.}}{k}\right)$, указанное в верхней половине табл. 4.

Далее, для расчета входящей в (II) вероятности $P_{прон.(1)}(T_{ост.(2)} = 11{,}95$ (час.)) будем исходить из аналогичного предположения, а поскольку $\frac{24-4}{11{,}95} \approx$ $\approx 1{,}67$ (раза), то при аналогичных рассуждениях будем иметь величину $P_{прон.(1)}(T_{ост.(2)} = 11{,}95$ (час.)), также указанную в верхней половине табл. 4.

Тогда, вычислив по формуле (II), имеем указанную в верхней половине табл. 4 величину интересующей вероятности $P_{прон.(2)}(T_{зад.} = 24$ (час.)).

Пусть также имеются исходные данные, приведенные наряду с $T_{зад.}$ для варианта 3 (причем $T_{диаг.}$, по аналогии с табл. 1 и табл. 2, включает при необходимости время восстановления целостности системы).

Результаты расчетов вероятности $P_{прон.(3)}(T_{зад.})$ для варианта 3 по (нижеследующей) формуле (III) утверждения III приведены в нижней половине табл. 4, причем с учетом выполненного его верхнего соотношения (*) индекс «*x*» для вероятности $P_{прон.(x)}(T_{ост.(3)})$ имеет значение «1», т. е. рассматриваем именно $P_{прон.(1)}(T_{ост.(3)})$ при $x = 1$.

***Утверждение III.*** Для варианта 3 при условии независимости исходных характеристик вероятность отсутствия источника опасности в системе за время $T_{зад.}$ равна:

$$P_{прон.(3)}(T_{зад.}) = \frac{N\cdot(T_{меж.}+T_{диаг.})}{T_{зад.}}\cdot P^{N}_{прон.(2)}(T_{меж.}+T_{диаг.}) + \\ + \frac{T_{ост.(3)}}{T_{зад.}}\cdot P_{прон.(x)}(T_{ост.(3)}), \qquad \text{(III)}$$

где $N = [T_{зад.} / (T_{меж.} + T_{диаг.})]$ — число периодов между диагностиками, целиком вошедших в $T_{зад.}$, остаток $T_{ост.(3)} = T_{зад.} - N\cdot(T_{меж.} + T_{диаг.})$,

$$x = \begin{cases} 1, & \text{если } T_{ост.3} < (T_{меж.} + T_{диаг.}) / k; \\ 2 & \text{— в противном случае.} \end{cases} \qquad (*)$$

Дадим некоторые пояснения к указанным в нижней половине табл. 4 вычисленным вероятностям $P_{прон.(2)}(T_{меж.} + T_{диаг.})$ и $P_{прон.(1)}(T_{ост.(3)})$, нужным для расчета по формуле (III) интересующей вероятности $P_{прон.(3)}(T_{зад.})$. Для входящей в (III) вероятности $P_{прон.(2)}(T_{меж.} + T_{диаг.})$ будем исходить из того естественного предположения, что за почти то же, что и $T_{зад.} = 24$ (час), время $T_{меж.} + T_{диаг.} = 23{,}9$ (час.) она практически не будет отличаться от ранее рассчитанной вероятности $P_{прон.(2)}(T_{зад.} = 24$ (час.)), т. е. примем $P_{прон.(2)}(T_{меж.} + T_{диаг.} = 23{,}9$ (час.)) $\approx$ $\approx P_{прон.}(T_{зад.} = 24$ (час.)).

А для промежуточного расчета также входящей в (III) вероятности $P_{прон.(1)}(T_{ост.3})$ при уже упомянутом выполненном верхнем неравенстве (*) будем исходить из того естественного предположения, что за меньшее время $T_{ост.(3)} = 0{,}1$ (час.) по сравнению с $T_{зад.} = 24$ (час.), для первого из которых в случае варианта 1 вероятность $\Omega_{возд.}(T_{зад.} - \tau)$ при $\tau \approx 4$ (час.) при полагаемой прямо пропорциональной зависимости ее от времени, уменьшится практически в $\frac{24-4}{0{,}1} \approx 200$ (раз), а вероятность $\int_0^{T_{зад.}} dA(\tau)$ (поскольку $\tau \ll T_{зад.}$) практически не изменится. Результат расчета интересующей вероятности $P_{прон.(3)}(T_{зад.})$ также приведен в нижней половине табл. 4.

Из всего вышесказанного ясно, что наиболее целесообразно использовать (по крайней мере, при весьма близких к рассмотренным значениям ключевых параметров) вариант 2 либо вариант 3 (характеризующиеся в рассматривавшемся для вероятного сетевого проникновения случае, но необязательно всегда, практически одинаковыми приближенными значениями вероятности отсутствия источника опасности в системе за время $T_{зад.}$).

Отметим, что вычисленное (с помощью MS Excel) значение риска ЧС в информатизированных котельных с сетевым доступом по формуле (2) $O_c$ при значениях всех остальных (т. е. кроме $O_{27}$, $O_{28}$) составляющих этой формулы, равных $Б_i = 0{,}5$, $O_i = 0{,}1$ при $P_{прон.(1)}(T_{зад.}) \approx (1 - O_{27}\cdot O_{28})_{(1)} \approx 0{,}699$, $P_{прон.(2)}(T_{зад.}) \approx (1 - O_{27}\cdot O_{28})_{(2)} \approx 0{,}819$, $P_{прон.(3)}(T_{зад.}) \approx$ $\approx (1 - O_{27}\cdot O_{28})_{(3)} \approx 0{,}819$ и рассмотренных значениях ключевых параметров данной технологии, т. е. многосменного мониторинга безопасности, составит

- для варианта 1: $O_c \approx 0{,}4527$;
- для варианта 2 и/или варианта 3: $O_c \approx 0{,}3587$.

Рассчитанные приближенные значения (хотя таковые получены далеко не для всех возможных величин параметров, учесть большую часть которых

при расчетах в той или иной степени представляется перспективным с помощью имитационного моделирования) говорят в пользу недопустимости игнорирования возможного сетевого проникновения внешнего злоумышленника (даже одного) в информатизированные котельные, чреватого возникновением в них ЧС.

Прикидочные расчеты показывают, что если бы при тех же значениях $Б_i = 0{,}5$, $O_i = 0{,}1$, всех остальных (т.е. кроме $O_{27}$, $O_{28}$) составляющих формулы (2) значение выражения $(1 - O_{27} \cdot O_{28})$, входящего в (2), удалось бы повысить до 0,990, то риск ЧС в информатизированной котельной с сетевым доступом по формуле (2) составил бы $O_c \approx 0{,}2248$, т.е. по сравнению с вариантом 1 при рассматривавшихся исходных данных и параметрах он снизился бы практически в 2 раза.

## Заключение

Хотя выполненные расчеты приблизительные, они все же дают представление и о том, какой или какие из трех рассмотренных вариантов технологии многосменного мониторинга безопасности наиболее целесообразно использовать при хотя бы близких к использовавшимся расчетным значениям, и о том, за счет изменения какого более предпочтительного из параметров соответствующего варианта данной технологии реально снизить риск ЧС для информатизированных котельных с сетевым доступом.

Так, в ракурсе технологии многосменного мониторинга безопасности системы для варианта 2 видится наиболее логичным и целесообразным снизить (регламентируемое) время $T_{меж.}$ между окончанием предыдущей и началом очередной диагностики целостности системы и/или увеличить количество смен между диагностиками системы, а для варианта 3 — снизить (регламентируемое) время $T_{меж.}$ между окончанием предыдущей и началом очередной диагностики целостности системы — при неизменном (заданном заказчиком) периоде $T_{зад.}$.

*Научная новизна* работы состоит в выясненной применимости существующей технологии многосменного мониторинга безопасности в качестве составляющей анализа и оценки по логико-вероятностной модели риска ЧС информатизированных котельных с сетевым доступом.

*Практическая ценность* работы заключается в:

- выявленном наиболее целесообразном варианте (а точнее, в двух выявленных наиболее целесообразных вариантах) технологии многосменного мониторинга безопасности для задаваемых конкретных значений ключевых параметров для трех рассмотренных вариантов для информатизированных котельных с сетевым доступом;
- способствовании анализу и расчету риска ЧС информатизированных котельных с сетевым доступом по построенной автором ранее логико-вероятностной модели, в т.ч. ***не*** исключая применение для этой цели имитационного моделирования для случаев неизвестных точных значений вероятностей инициирующих событий и инициирующих условий.

Основа работы была выполнена автором в Финансовом университете после (успешной) аттестации в должности доцента и продолжена в период пребывания слушателем курсов повышения квалификации НИУ «Высшая школа экономики».

Автор признателен организаторам Всероссийской научно-практической конференции «Человек, общество и государство в обеспечении безопасности жизнедеятельности современной России», особенно ее круглого стола «Современные методы мониторинга опасных явлений как основа анализа риска» за предоставленную возможность выступления с указанной тематикой и опубликования материалов данной работы.

## Литература [References]

1. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» (с изменениями и дополнениями). [Federal law of 21 July 2011 № 256-FL "About safety of objects of fuel-energy complex" (with changes and additions).]
2. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». [ISO/IEC 27002:2012. Information technology. Security techniques. Code of practice for information security management.]
3. Корт С.С. Теоретические основы защиты информации: Учеб. пособие. М.: Гелиос АРВ, 2004. 240 с. [Court S.S. Theoretical foundations of information security: the training manual. Moscow: Helios ARV, 2004. 240 p.]

4. Костогрызов А.И., Петухов А.В., Щербина А.М. Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа. М.: Вооружение. Политика. Конверсия, 1994. 278 с. [Kostogryzov A.I., Petukhov A.V., Shcherbina A.M. The basis of evaluation, providing and improving the quality of output information in MIS of the organizational type. M.: Weapon. Policy. Conversion, 1994. 278 p.]
5. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003. 368 с. [Melnikov V.V. Information security in automated systems. M.: Finance and statistics, 2003. 368 p.]
6. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000. 248 с. [Ryabinin I.A. Reliability and safety of structural-complex systems. SPb.: Polytechnic, 2000. 248 p.]
7. Соколов Ю.И. Новый вид рисков: риски киберпространства // Проблемы анализа риска. 2016. Т. 13. № 6. С. 6—21. [Sokolov Yu. I. A new type of risks: cyber risks // Issues of risk analysis. 2016. V. 13. No. 6. P. 6—21.]
8. Шептунов М.В. Котельные как информатизируемые объекты защиты в ракурсе надежности и безопасности структурно-сложных систем // Проблемы анализа риска. 2018. Т. 15. № 1. С. 80—88. [Sheptunov M.V. Boiler-houses as the computerized objects of protection at foreshortening of reliability and safety of structural-complex systems // Issues of risk analysis. 2018. V. 15. No. 1. P. 80—88.]

## Сведения об авторе

**Шептунов Максим Валерьевич:** кандидат технических наук, доцент, член Ученого совета Института информационных наук ФГБОУ ВО «Московский государственный лингвистический университет» (МГЛУ), доцент ФГБОУ ВО «Российский государственный гуманитарный университет» (РГГУ)

Количество публикаций: св. 60, в т.ч. глава в двух коллективных монографиях, более 20 вышеупомянутых работ — учебно-методические

Область научных интересов: исследование операций, управление в социально-экономических и технических системах, дискретный анализ и анализ риска

*Контактная информация:*

Адрес: 129347, г. Москва, ул. Проходчиков, 5-23

Тел.: +7 (915) 297-22-75

E-mail: triumf403@yandex.ru