УДК 519.8:614.838+510.6:62-7:007.51:004.056.53

Котельные как информатизируемые объекты защиты в ракурсе надежности и безопасности структурно-сложных систем

ISSN 1812-5220

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

Аннотация

Обсуждаются некоторые вопросы и особенности котельных, в том числе муниципальных образований, с позиции теории безопасности структурно-сложных систем: как объектов защиты от физического и компьютерного (сетевого) несанкционированного доступа (НСД), так и риска аварии, вероятными последствиями которых являются взрыв либо иное состояние котельной, проявляющееся в существенном отклонении от нормального режима функционирования. На основе логических построений сформирован возможный сценарий опасного состояния системы, в котором предполагается НСД одного нарушителя с возможностью сопутствующего ему отказа подсистемы контроля доступа и/или подсистемы охранной сигнализации котельной либо подсистемы защиты информации последней. Получена логико-вероятностная модель, в том числе расчетная формула для риска указанной чрезвычайной ситуации.

Ключевые слова: безотказность, взрыв котельной, логико-вероятностный метод, несанкционированный доступ, ограничение доступа, отказ, подсистема, риск, система обнаружения вторжений.

Содержание

Введение

В настоящее время интеграция систем физической и информационной безопасности котельных муниципальных образований, как и других объектов, представляющих интерес в стратегическом плане, является одним из перспективных направлений развития современных интегрированных систем безопасности (ИСБ) предприятия.

Среди ключевых звеньев практически любой современной котельной важно выделить, в том числе, автоматизированное рабочее место (АРМ) оператора. Поскольку АРМ чаще всего создается на базе подключаемых к локальным и глобальной сетям персональных компьютеров, представляя собой 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.

Весьма актуальные в ракурсе информационно-телекоммуникационных технологий вопросы рисков использования киберпространства, включая автоматизированные системы управления технологическими процессами, рассматривались в различных источниках, в том числе и на страницах журнала «Проблемы анализа риска» [9 и др.].

Хотя существовали и будут иметь место отдельные задачи, которые успешно и эффективно решаются узкоспециализированными подсистемами, такими как аппаратура и программное обеспечение для защиты периметра, контроля и управления доступом (КУД), теле- и видеонаблюдения, охранной сигнализации, пожарной сигнализации, контроля за утечкой газа (газов), следует отметить возрастающий выбор именно ИСБ, использование которых позволяет не только решить возникающие задачи обеспечения безопасности в комплексе, но и повысить эффективность работы отдельных подсистем, входящих в систему.

Среди основных защищаемых, но уязвимых целей при рассмотрении безопасности котельных следует отметить: персонал предприятия, материальные ресурсы (имущество, высоколиквидное сырье и пр.), информационные ресурсы (информация на носителях и информация, циркулирующая по внутренним каналам компании, и проч.). Кроме существенных организационных мер, принимаемых для котельных, важно отметить и технические меры. Помимо защиты собственно от несанкционированного доступа к системе это и резервирование особо важных компьютеризованных подсистем, и установка оборудования обнаружения и тушения пожара, как и обнаружения утечек воды, и принятие конструктивных мер защиты от хищений, взрывов, и установка резервных источников электропитания, и оснащение помещений замками, теми либо иными разновидностями сигнализации и многое другое.

В определенных случаях ущерб, причиненный одному или нескольким ресурсам, произошедший либо вследствие аварии, либо в результате злоумышленных или неумышленных действий персонала либо иных лиц может оказаться фатальным для жизнедеятельности предприятия и даже привести к его ликвидации или банкротству, поскольку так или иначе котельные муниципальных образований представляют собою объекты экономики и народного хозяйства.

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

Отметим, что рассматриваемая сфера регулируется в основном федеральным законом [1], статья 7 которого «Требования обеспечения безопасности объектов топливно-энергетического комплекса и требования антитеррористической защищенности объектов топливно-энергетического комплекса» прямо указывает на необходимость защиты от террористических воздействий объектов топливно-энергетического комплекса. В свою очередь, в статьях 9 и 11 «Система физической защиты объектов топливно-энергетического комплекса» и «Обеспечение безопасности информационных систем объектов топливно-энергетического комплекса» того же ФЗ [1] говорится соответственно о системе физической защиты и безопасности информационных систем вышеупомянутых объектов.

Представляется существенным и то, что ряд ключевых понятий, используемых в области управления физическим доступом, играет не менее важную роль в сфере объектов информационной безопасности (например, термины, «идентификация», «идентификатор», «разграничение полномочий»).

Хотя рассмотрение ГОСТов и нормативных документов не является целью данной работы, на всякий случай упомянем, что ряд государственных стандартов, включая международные и межгосударственные, имеет отношение к безопасному функционированию котельных муниципальных образований, среди которых сложно проигнорировать в ракурсе злоумышленных и неумышленных действий тех или иных лиц стандарты [2–6].

В данной работе, не претендующей на полноту исследования различных аспектов функционирования котельных муниципальных образований, цель

ставится следующим образом: рассмотреть лишь некоторые, представляющиеся принципиально важными в ракурсе безопасного функционирования, вопросы анализа и оценки риска чрезвычайной ситуации для вышеупомянутых информатизируемых объектов топливно-энергетического комплекса.

В общем случае, в ракурсе логико-вероятностного подхода (о котором более подробно см., например, [8]) к формулируемой и решаемой в данной работе научно-практической задаче, выражение для вероятностной функции опасности системы имеет вид:

$$O_c = P\{f(z_1,...,z_m) = 1\}, \qquad (1)$$

где O_c — вероятность опасности системы;

z_1, ..., z_m — инициирующие события и условия (ИС, ИУ), причем

$$z_i = \begin{cases} 1, \text{если ИС (ИУ) } z_i \text{ произошло (возникло)}, \\ 0 \text{ — если ИС (ИУ) } z_i \text{ не произошло} \\ \quad \text{(не возникло)}. \end{cases}$$

Аналогично имеют место соотношения

$$O_i = P\{z_i = 1\},$$

$$Б_i = P\{z_i^{'} = 1\},$$

где O_i — вероятность опасности от ИС (ИУ) z_i;

$Б_i$ — вероятность безопасности от наличия ИС (ИУ) z_i;

$z_i^{'}$ — отрицание ИС (ИУ) z_i, где $i = \overline{1,m}$.

Определение 1. *Вероятностной функцией (ВФ)* называется вероятность истинности функции алгебры логики (ФАЛ)

$$P\{f(z_1,...,z_m) = 1\}.$$

Определение 2. Функции алгебры логики, допускающие непосредственный переход к ВФ заменой логических переменных вероятностями, а логических операций — соответствующими арифметическими операциями, называются *формами перехода к замещению* (ФПЗ).

Отметим, что частным случаем ФПЗ является форма перехода к полному замещению (ФППЗ), когда имеет место замещение одновременно всех логических переменных.

Определение 3. Функция, записанная в виде матрицы, в которой конъюнкции обозначены расположением логических символов в строке, а дизъюнкции — расположением их в столбце, называется *логической матрицей*.

Важно подчеркнуть, что к логической матрице применимы все известные преобразования алгебры логики.

Известно [8 и др.], что переход к ВФ для ФАЛ, представленной в ФППЗ, осуществим по определенным правилам, причем вероятностную функцию для ФАЛ, представленной в произвольной бесповторной форме, возможно найти по ее выражению в базисе конъюнкция-отрицание. Последнее получается путем многократного применения правила (закона) де Моргана.

В настоящей работе научно-практическая задача, разбиваемая на две подзадачи, формулируется следующим образом:

- сформировать сценарий опасного состояния, а именно сценарий возникновения чрезвычайной ситуации для котельных муниципальных образований;
- получить на основе логико-вероятностного метода расчетную формулу для числовой оценки риска чрезвычайной ситуации в котельной муниципального образования.

1. Сценарий опасного состояния

За чрезвычайную ситуацию, происходящую с подлежащей далее расчету вероятностью, в данной работе был принят взрыв в котельной (либо иное ее состояние, проявляющееся в существенном отклонении от нормального режима функционирования).

Отметим, что в формируемом здесь сценарии опасного состояния (СОС) 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 сложные события z_{27} и z_{29}). Всего из весьма большого перечня возможных по своей сути ИС и ИУ были включены в сценарий опасного состояния 32 ИС и ИУ, в том числе 18 ИС и 14 ИУ, как показано на рисунке.

Данным СОС системы предполагается НСД одного нарушителя в результате преодоления защитной физической «суммарной» преграды (включая возможное проникновение под видом должностного либо иного лица или совместно с ним) с учетом возможности совместимого отказа подсистемы охранной сигнализации и/или контроля и управ-

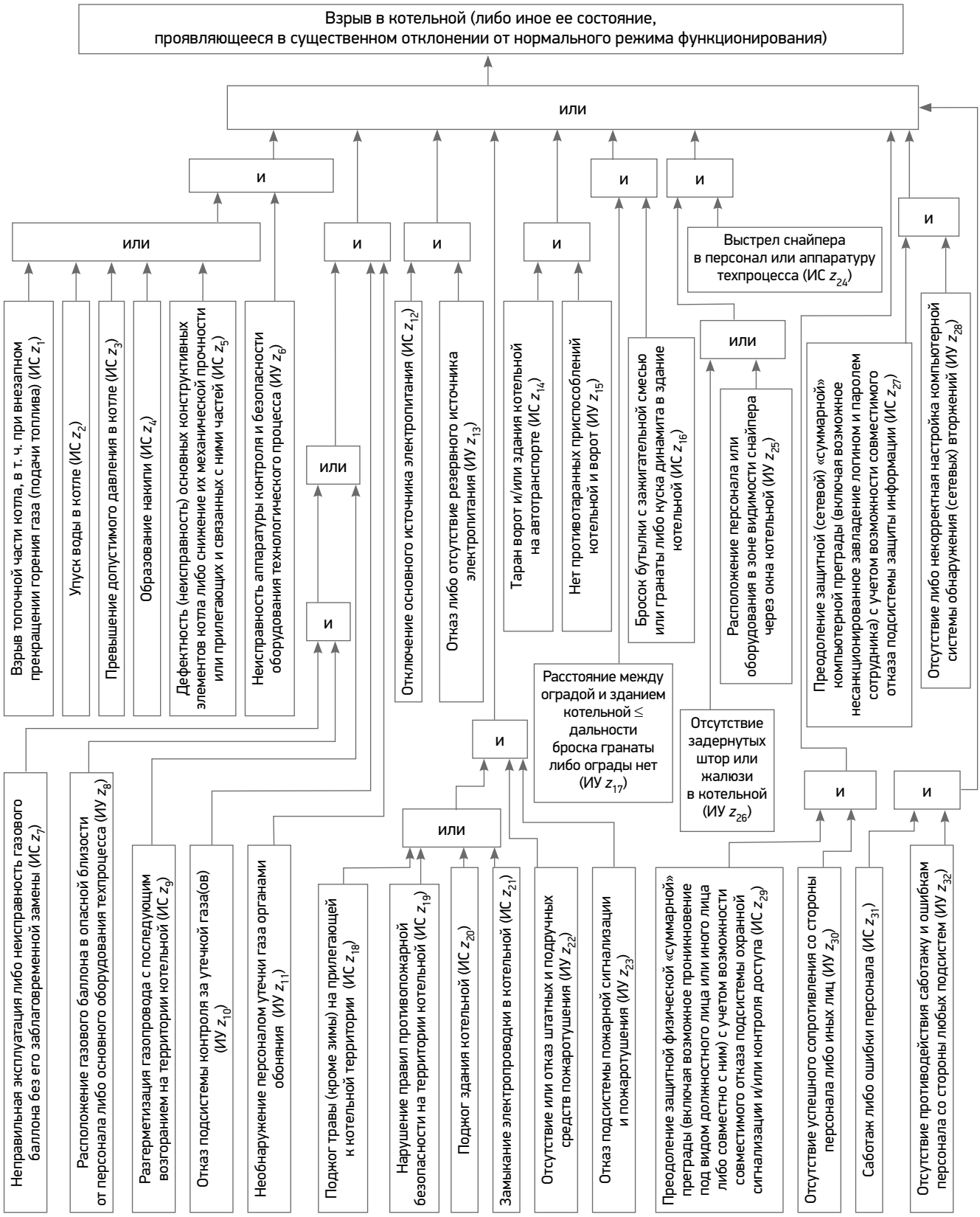

Рисунок. Возможный сценарий опасного состояния котельной

ления доступом (сложное инициирующее событие z_{29}). Аналогично предполагается (удаленный) НСД единственного нарушителя (к АРМ оператора котельной и содержащейся на нем защищаемой информации) в результате преодоления защитной (сетевой) «суммарной» компьютерной преграды (включая возможное несанкционированное завладение логином и паролем сотрудника котельной) с учетом возможности совместимого отказа подсистемы защиты информации котельной (сложное инициирующее событие z_{27}).

Для ИС z_{31} и ИУ z_{32} предполагается, что упомянутые для них ошибки персонала котельной не являются взаимоисключающими.

Отметим, что ИС z_1, …, z_5, как и сопутствующее им ИУ z_6, фигурирующие в СОС системы, относятся (если формулировать это таким образом) к организационно-техническим неисправностям основного оборудования технологического процесса; к этой же категории можно было бы отнести и ИС z_{31} и ИУ z_{32}. Часть ИС и ИУ, а именно z_{27}, z_{28}, относится к возможностям удаленных (сетевых) атак на котельную, являющуюся информатизируемым объектом. Не оставим без внимания и то, что заметная часть ИС и ИУ, помимо также ощутимой части относящихся к пожаровзрывобезопасности и/или утечек газа (газов) ИС и ИУ, присутствующая в СОС, относится к (локальному) НСД и вопросам надежности как отдельных подсистем, так и системы в целом.

Некоторые принципиальные подробности, относящиеся к рассмотрению отдельных ИС (в частности, к z_{27}, z_{29}) и их происхождению, изложены в следующем разделе статьи.

2. Логико-вероятностная модель для оценки риска и повышения надежности и безопасности

Поскольку сценарий опасного состояния системы получен и рассмотрен в разделе 1 (см. рисунок), возможно записать соответствующую ему логическую матрицу.

Так как последняя, формируемая на основе СОС системы, не содержит повторяющихся переменных, сможем перейти с учетом определений 1—3 и других нужных сведений введения данной работы от ФАЛ к ВФ.

Преобразовывая сначала с помощью закона коммутативности, а также закона де Моргана, записываемого в виде

$$\bigvee_{i=1}^{n} z_i = \left(\bigwedge_{i=1}^{n} z_i' \right)'$$

(где штрих означает инверсию), получим:

$$f(z_1,\ldots,z_{32}) = \left| \begin{array}{l|l} z_1 z_2 z_3 z_4 z_5 & z_6 \\ z_7 z_8 z_9 & z_{10} z_{11} \\ z_{12} z_{13} \\ z_{14} z_{15} \\ z_{16} z_{17} \\ z_{18} z_{19} z_{20} z_{21} & z_{22} z_{23} \\ z_{24} & z_{25} \\ & z_{26} \\ z_{27} z_{28} \\ z_{29} z_{30} \\ z_{31} z_{32} \end{array} \right| =$$

$$= (z_1 \vee z_2 \vee z_3 \vee z_4 \vee z_5)\, z_6 \vee (z_7 z_8 \vee z_9)\, z_{10} z_{11} \vee z_{12} z_{13} \vee$$

$$\vee z_{14} z_{15} \vee z_{16} z_{17} \vee (z_{18} \vee z_{19} \vee z_{20} \vee z_{21})\, z_{22} z_{23} \vee z_{24}(z_{25} \vee z_{26}) \vee$$

$$\vee z_{27} z_{28} \vee z_{29} z_{30} \vee z_{31} z_{32} = z_6(z_1 \vee z_2 \vee z_3 \vee z_4 \vee z_5) \vee$$

$$\vee z_{24}(z_{25} \vee z_{26}) \vee z_{22} z_{23}(z_{18} \vee z_{19} \vee z_{20} \vee z_{21}) \vee z_{10} z_{11}(z_9 \vee z_7 z_8) \vee$$

$$\vee z_{12} z_{13} \vee z_{14} z_{15} \vee z_{16} z_{17} \vee z_{27} z_{28} \vee z_{29} z_{30} \vee z_{31} z_{32} =$$

$$= z_6\left(z_1' z_2' z_3' z_4' z_5'\right)' \vee z_{24}\left(z_{25}' z_{26}'\right)' \vee z_{22} z_{23}\left(z_{18}' z_{19}' z_{20}' z_{21}'\right)' \vee$$

$$\vee z_{10} z_{11}[z_9'(z_7 z_8)']' \vee z_{12} z_{13} \vee z_{14} z_{15} \vee z_{16} z_{17} \vee z_{27} z_{28} \vee$$

$$\vee z_{29} z_{30} \vee z_{31} z_{32} = \left\{[z_6\left(z_1' z_2' z_3' z_4' z_5'\right)']' \wedge [z_{24}\left(z_{25}' z_{26}'\right)']' \wedge \right.$$

$$\left. \wedge [z_{22} z_{23}\left(z_{18}' z_{19}' z_{20}' z_{21}'\right)']' \wedge \{z_{10} z_{11}[z_9'(z_7 z_8)']'\}' \wedge (z_{12} z_{13})' \wedge \right.$$

$$\left. \wedge (z_{14} z_{15})' \wedge (z_{16} z_{17})' \wedge (z_{27} z_{28})' \wedge (z_{29} z_{30})' \wedge (z_{31} z_{32})'\right\}'. \quad (2)$$

Затем по известным правилам, учитывая, что ФАЛ (2) является бесповторной, перейдем от нее

непосредственно к интересующей вероятностной функции опасного состояния (ФОС) системы:

$$P\{f(z_1,\ldots,z_{32})=1\}=1-\{[1-O_6(1-Б_1Б_2Б_3Б_4Б_5)]\times$$
$$\times[1-O_{24}(1-Б_{25}Б_{26})]\times[1-O_{22}O_{23}(1-Б_{18}Б_{19}Б_{20}Б_{21})]\times$$
$$\times\{1-O_{10}O_{11}(1-[Б_9(1-O_7O_8)])\}\times(1-O_{12}O_{13})\times$$
$$\times(1-O_{14}O_{15})\times(1-O_{16}O_{17})\times(1-O_{27}O_{28})\times(1-O_{29}O_{30})\times$$
$$\times(1-O_{31}O_{32})\}. \quad (3)$$

Результат формальной проверки при подстановке в (3) одинаковых вероятностей $O_i = O_1 = O_2 = \ldots = O_{31} = O_{32} = 1$ дает:

$$P\{f(z_1,\ldots,z_{32})=1\}=1-0=1,$$

позволяя утверждать о правильности выполненных ранее преобразований; при вероятностях $O_i = 1$ каждого из соответствующих инициирующих событий и инициирующих условий указанная в сценарии опасного состояния системы чрезвычайная ситуация неизбежно произойдет (с вероятностью $O_c = 1$).

Рассмотрим следующий числовой *пример* (с условными значениями вероятностей O_i и $Б_i$), а именно пусть: $Б_1 = \ldots = Б_5 = Б_9 = Б_{18} = \ldots = Б_{21} = Б_{25} = Б_{26} = 0{,}5$; $O_6 = \ldots = O_8 = O_{10} = \ldots = O_{17} = O_{22} = \ldots = O_{24} = O_{27} = \ldots = O_{32} = 0{,}1$. Тогда вычисление (в MS Excel) по формуле (3) дает (с округлением): $O_c \approx 0{,}2248$.

В данном условном примере интересующая вероятность O_c не является почти равной единице, но и не является почти равной нулю, как не является она равной и значению 0,5.

Естественно, что для как такового расчета риска рассматриваемой чрезвычайной ситуации нам нужны вероятности каждого из ИС и ИУ, входящих в формулу (1), а в рассматриваемом нами случае и в формулу (2). Для их использования могли бы помочь статистические данные (при наличии последних). Нетривиальной и важной задачей представляется определение соответствующих вероятностей опасности для составляющих O_{27}, O_{29} вышеуказанной формулы.

Обозначим прочности (частично) перекрывающих друг друга преград (для многозвенной защиты) в общем случае через P_1, P_2, P_3,…, P_n. Вероятность преодоления каждой из них (единственным) нарушителем согласно теории вероятностей как противоположное событие может быть выражена как соответствующая разность $(1 - P_1)$, $(1 - P_2)$, $(1 - P_3)$, …, $(1 - P_n)$.

В ракурсе ИС z_{29}, например, этими преградами при наличии на них охранной сигнализации и/или контроля доступа могут быть помимо ворот внешней ограды дверь здания котельной и окна котельной. Считая (еще до рассмотрения всей совокупности независимых ИС и ИУ z_1, …, z_{32}, где z_{27}, z_{29} — события сложные, в сценарии опасного состояния и его как такового формирования) факты преодоления этих приведенных в качестве примера для ИС z_{29} преград событиями совместимыми, вероятность преодоления «суммарной» преграды нарушителем запишем в виде

$$P_{\text{нр}} = (1 - P_1) \times (1 - P_2) \times (1 - P_3) \times \ldots \times (1 - P_i), \quad (4)$$

где $i = \overline{1,n}$; смысл обозначений соответствует вышеуказанному.

Чтобы определить интересующую вероятность O_{29}, имеет смысл до применения данной достаточно общей формулы (4) принимать во внимание справедливость выражения для прочности (т.е. вероятности непреодоления) многозвенной защиты с контролируемыми преградами для защиты от одного нарушителя [7] (в данном рассматриваемом случае полагалось, как вариант, $P_{\text{нр}} = O_{29}$, что аналогично далее можно было бы записать при тех же рассуждениях для O_{27}), а именно прочность контролируемой защиты

$$P_{\text{зик}} = P_i = \min\{(P_{\text{облк1}} \times (1 - P_{\text{откк1}})),$$
$$(P_{\text{облк2}} \times (1 - P_{\text{откк2}})), \ldots, (P_{\text{облк}n} \times (1 - P_{\text{откк}n})),$$
$$(1 - P_{\text{обх1}}), (1 - P_{\text{обх2}}), \ldots, (1 - P_{\text{обх}j})\}, \quad (5)$$

где $P_{\text{облк}n}$ — вероятность обнаружения и блокировки НСД при попытке преодоления нарушителем n-й преграды;

$P_{\text{откк}n}$ — вероятность отказа техники при контроле (обнаружении и блокировке НСД) n-й преграды;

$P_{\text{обх}j}$ — вероятность обхода преграды по j-му пути.

Иными словами, прочность многозвенной защитной оболочки от единственного нарушителя равна прочности ее слабейшего звена.

Так, например, если одно из (пусть всего двух) окон котельной, являясь контролируемой преградой с вероятностью ее преодоления P_3, меньшей по отношению к вероятностям преодоления другого окна P_2 и единственной двери здания P_1, перекрывается внешней оградой здания с вероятностью ее преодоления P_4, то следует использовать в формуле (4) получаемое таким образом по формуле (5)

минимальное значение, а именно P_3, при предварительном применении только что указанной формулы, т.е. тогда бы формула (4) с учетом (5) имела бы вид: $P_{\text{нр}} = (1 - P_4) \times (1 - P_3)$.

В свою очередь,

$$P_{\text{облкл}} = \frac{t_{\text{нр}}}{T_{\text{обл.}}},$$

где $t_{\text{нр}}$ — время преодоления (контролируемой) преграды нарушителем;

$T_{\text{обл.}}$ — время обнаружения и блокировки НСД, из чего вытекает справедливость формулы для вероятности преодоления (отдельной) преграды нарушителем

$$P_{\text{нр}} = 1 - \frac{t_{\text{нр}}}{T_{\text{обл.}}}.$$

В наиболее простом (но далеко не единственно возможном для котельной случае) вероятность отказа интересующей подсистемы (учитываемая в формуле (5)) обычно определяется по следующей формуле, также упоминаемой в [7],

$$P_{\text{отк}}(t) = e^{-\lambda t}, \qquad (6)$$

где λ — интенсивность отказов группы технических средств, составляющих подсистему (систему) обнаружения и блокировки НСД;

t — рассматриваемый интервал времени функционирования подсистемы (системы) обнаружения и блокировки НСД.

Аналогичным образом имеет смысл поступать для определения другой интересующей вероятности опасности O_{27}.

Отметим, что (в данном рассмотрении простые) события $P_1, P_2, P_3, \ldots, P_n$ полагаются также (хотя и совместимыми друг с другом, но) независимыми как по отношению друг к другу, так и по отношению к любым ИС и ИУ, фигурирующим в СОС системы (кроме, в свою очередь, соответствующих фигурирующих в СОС сложных событий, например, z_{27}, зависящее от относящихся только к нему простых событий $P_{1z_{27}}, P_{2z_{27}}, \ldots, P_{nz_{27}}$, и z_{29}, зависящее от относящихся только к нему простых событий $P_{1z_{29}}, P_{2z_{29}}, \ldots, P_{nz_{29}}$).

Подразумевается, что для соответствующих случаев резервирования подсистем могут и должны использоваться более сложные (по сравнению с формулой (6)) адекватные им совокупности формул показателей теории надежности.

Для анализа и управления риском (и в том числе для решения вопросов о резервировании, не являющихся основным предметом рассмотрения данной статьи) имеют смысл рассчитываемые критерии: значимость того или иного элемента (либо имеющейся подсистемы) системы и соответствующий вес его (ее) в последней. Как известно, критерий «веса» характеризует положение элемента (либо, как вариант, подсистемы) в структуре системы и не зависит от надежностных показателей, а «значимость» элемента определяется не только местом элемента (либо, как вариант, подсистемы) в структуре системы, но и надежностью всех других элементов, кроме самого x_i.

«Вес» интересующего элемента x_i в системе возможно рассчитать по известной формуле

$$g_{x_i} = \sum_{f=1}^{k} 2^{-(r_f - 1)} - \sum_{j=1}^{l} 2^{-(r_j - 1)},$$

где k, r_f — число и ранг ортогональных конъюнкций, содержащих аргумент x_i;

l, r_j — число и ранг ортогональных конъюнкций, содержащих отрицание элемента x_i' (где штрих означает инверсию), —

имея выражение (2), записанное в дизъюнктивной нормальной форме (ДНФ). Нередко для этой цели используют алгоритм ортогонализации, сводя ДНФ к ОДНФ [8].

Если значения вероятностей, входящих в формулу для расчета риска, неизвестны, то соответственно структурную значимость элемента x_i можно определить, взяв частную производную

$$B(i) = \left.\frac{\partial R_c}{\partial R_i}\right|_{R_1 = \ldots = R_m = 0,5},$$

с подстановкой вероятностей безотказной работы всех элементов, равных значению 0,5, в выражение для надежностной значимости аргумента x_i'

$$B(i \setminus R) = \frac{\partial R_c}{\partial R_i},$$

где $R_c = f(R_1, \ldots, R_m)$ — вероятность безотказной работы системы, зависящая и от вероятности безотказной работы i-го элемента R_i, где $i = \overline{1,m}$ (когда вероятности безотказной работы для каждого элемента системы известны, возможно применить непосредственно последнее общего вида выражение).

Напомним, что соотношение вида $R_c = 1 - Q_c$ (а в соответствующих нашему случаю обозначениях с учетом (3) $Б_c = 1 - О_c$) связывает вероятность безотказной (безопасной) работы системы с вероятностью отказа (опасности) системы.

Следует также отметить, что не представляют особых трудностей расчеты и для лиц, не являющихся профессиональными программистами, в (имеющемся почти на каждой персональной ЭВМ) MS Excel с его строкой формул; как по данной логико-вероятностной модели риска, так и для такого рода структурных моделей близких по сущности объектов — даже если в них появятся повторные инициирующие события и/или условия.

Заключение

Итак, *научная новизна* данной *работы* состоит в следующем:

- сформирован путем логических построений сценарий опасного состояния для котельных, в том числе муниципальных образований;
- получена на основе логико-вероятностного метода расчетная формула числовой оценки риска чрезвычайной ситуации котельных муниципальных образований.

Практическая ценность работы заключается:

- в принципиальной возможности числовой оценки риска чрезвычайной ситуации в котельной муниципального образования по полученной расчетной формуле;
- при выяснении степени влияния каждого из инициирующих событий и инициирующих условий на вероятность рассматриваемой чрезвычайной ситуации в возможности снизить риск последней за счет снижения вероятностей наиболее опасных из них как техническими, так и организационными мероприятиями.

Следует отметить, что поскольку изначально в данной работе предполагалась наряду с преодолением защитной физической «суммарной» преграды возможность совместимого отказа подсистемы охранной сигнализации и/или контроля и управления доступом (в сценарии опасного состояния фигурирует сложное инициирующее событие z_{29}, являющееся независимым по отношению к каждому из всех других присутствующих в данном сценарии 32 ИС и ИУ; аналогично для сложного ИС z_{27}, все ИС и ИУ $z_1,...,z_{32}$ предполагаются независимыми попарно и в совокупности), представляет интерес в плане дальнейших исследований каждая из двух возможных последующих постановок научно-практических задач:

1) максимизация надежности соответствующей подсистемы при задаваемом уровне финансовых ограничений на стоимость данной подсистемы

либо

2) минимизация стоимости соответствующей подсистемы при требуемом уровне надежности данной подсистемы.

Обе они, внося свой вклад в уменьшение риска чрезвычайной ситуации в целом в котельной, могут иметь значение также и для предусматривавшегося изначально наряду с преодолением защитной (сетевой) компьютерной преграды возможного случая совместимого отказа подсистемы защиты информации (сложное ИС z_{27} по аналогии с ИС z_{29}). Актуальны обе указанные задачи и соответственно для подсистемы пожарной сигнализации и подсистемы контроля за утечкой газа (газов) в котельных.

Эти задачи могут быть успешно решены хорошо разработанными на сегодняшний день методами классической теории надежности, а именно для разновидностей подсистем: резервированных невосстанавливаемых, резервированных восстанавливаемых (подсистем либо систем).

Основная часть данной 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 «Устойчивость муниципальных образований к чрезвычайным ситуациям» за предоставленную возможность публикации в качестве дополняющего материала данной работы в журнале.

Литература

1. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» (с изменениями и дополнениями).
2. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения без-

опасности. Свод норм и правил менеджмента информационной безопасности».
3. ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
4. ГОСТ Р 54831-2011 «Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний».
5. ГОСТ 26342-84 «Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры».
6. ГОСТ 27990-88 «Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования».
7. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003. 368 с.
8. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000. 248 с.
9. Соколов Ю.И. Новый вид рисков — риски киберпространства // Проблемы анализа риска. 2016. Т. 3. № 6. С. 6—21.

Сведения об авторе

Шептунов Максим Валерьевич: кандидат технических наук, доцент, член Ученого совета факультета «Международная информационная безопасность» ФГБОУ ВО «Московский государственный лингвистический университет (МГЛУ), доцент ФГБОУ ВО «Российский государственный гуманитарный университет» (РГГУ)

Количество публикаций: св. 60 учебно-методических и научных работ, в т. ч. глава в двух коллективных монографиях, в одной из которых являлся зам. руководителя авторского коллектива, более 20 вышеупомянутых работ — учебные (учебно-методические) издания

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

Контактная информация:

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

Тел.: +7 (915) 297-22-75

E-mail: triumf403@yandex.ru