УДК 626/627.8:001.5:519.7

ВЕРОЯТНОСТНОЕ МОДЕЛИРОВАНИЕ ГИПОТЕТИЧЕСКИХ СЦЕНАРИЕВ ДВУХ НЕТИПОВЫХ АВАРИЙ НА ГИДРОЭНЕРГЕТИЧЕСКИХ ОБЪЕКТАХ ПРИ ОТКАЗАХ АВТОМАТИКИ

Стефанишин Дмитрий Владимирович
Ведущий научный сотрудник Института телекоммуникаций и глобального информационного пространства Национальной академии наук Украины, г.Киев, доктор технических наук

Романчук Екатерина Геннадиевна
Аспирантка Института телекоммуникаций и глобального информационного пространства Национальной академии наук Украины, г.Киев

За последнее десятилетие на объектах гидроэнергетики произошло несколько аварий, которые можно назвать нетиповыми, поскольку раньше подобные аварии в мировой практике еще не случались [1-6]. Ход этих аварий сопровождался отказами автоматических средств контроля и регулирования, оснащенных современной компьютерной техникой.

Одна из таких аварий произошла 14 декабря 2005 г. на ГАЭС Таум Саук (Taum Sauk, штат Миссури, США). В результате аварии разрушилась дамба ограждения верхового бассейна ГАЭС (рис. 1).

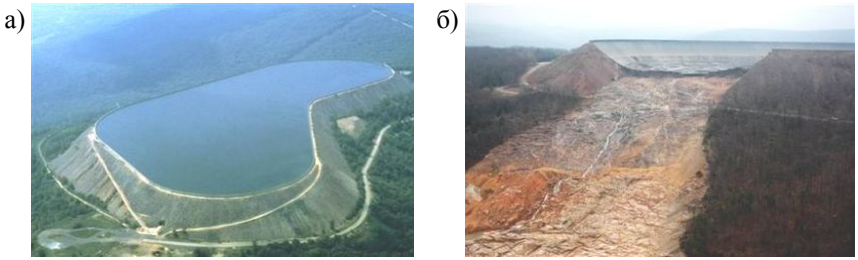

Рис. 1. Верховой бассейн ГАЭС Taum Sauk (США) до (а) и после аварии (б) в 2005 г.

По результатам расследования аварии было установлено, что причинами разрушения дамбы ограждения верхового бассейна ГАЭС Taum Sauk были его переполнение и перелив воды через гребень дамбы вследствие сбоя в компьютерной программе системы автоматического регулирования уровня воды в бассейне [1, 2].

Другая авария произошла 17 августа 2009 года на Саяно-Шушенской ГЭС (Россия, Хакассия) в результате разгерметизации напорного тракта и разрушения одного из гидроагрегатов (рис. 2).

а) б)

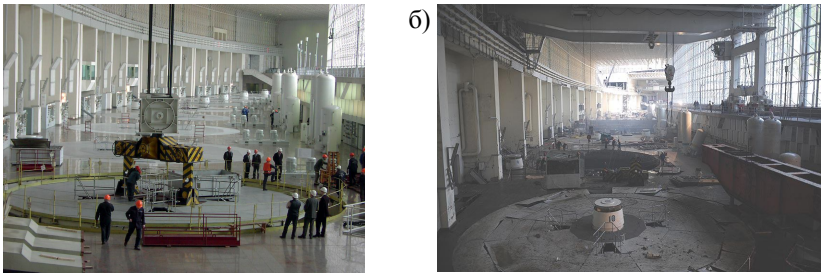

Рис. 2. Машинный зал Саяно-Шушенской ГЭС
до (а) и после аварии (б) 2009 г.

Авария получила катастрофическое развитие вследствие отказа автоматики, которая не сработала в режиме перекрытия напорного тракта аварийно-ремонтным затвором. При аварии погибло 75 работников ГЭС [3, 4].

В обоих случаях аварии носили сложный системный характер с вовлечением в механизмы их возникновения и развития отказов автоматических средств обеспечения безопасности объектов.

С целью установления роли автоматических средств контроля и регулирования в ходе аварий на ГАЭС Taum Sauk (2005 г.) и на Саяно-Шушенской ГЭС (2009 г.) авторами было осуществлено вероятностное моделирование гипотетических сценариев развития аварий с учетом отказов систем автоматики и произведены расчеты вероятностей аварий при разных значениях вероятностей отказов автоматических устройств.

При моделировании и оценке вероятности аварии на ГАЭС Taum Sauk рассматривались система $\mathbf{S}_{1,a} = \{s_d, s_a\}$ в составе оградительной дамбы верхового бассейна (подсистема s_d) и системы автоматического регулирования уровня воды в бассейне (подсистема s_a).

Принимались следующие обозначения для вероятностей аварийных событий: $P(s_d)$ – вероятность разрушения дамбы по независимым от работы автоматики причинам (вероятность отказа подсистемы s_d); $P(s_a)$ – вероятность отказа системы автоматического регулирования уровня (вероятность отказа подсистемы s_a).

Авария на верховом бассейне ГАЭС Taum Sauk могла бы и не состояться, если бы в оригинальном проекте на случай отказа автоматики был предусмотрен аварийный водослив. Работоспособность аварийного водослива в системе при отказе подсистемы автоматического регулирования моделировалась условием θ. Вероятность разрушения дамбы при этом условии обозначена как $P(s_{d,\theta})$.

Пусть $\overline{\theta}$ – условие безотказной работы подсистемы автоматического регулирования в системе $\mathbf{S}_{1,a} = \{s_d, s_a\}$; $\left(\mathbf{S}_{1,a}, \overline{\theta}\right)$ – аварийное событие в системе $\mathbf{S}_{1,a}$ при условии $\overline{\theta}$; $\left(\mathbf{S}_{1,a}, \theta\right)$ – то же при условии θ.

Условия θ, $\overline{\theta}$, по определению, формируют полную группу событий. Следовательно, события $\left(\mathbf{S}_{1,a}, \overline{\theta}\right)$, $\left(\mathbf{S}_{1,a}, \theta\right)$ являются несовместными, и полная вероятность аварии в системе $\mathbf{S}_{1,a}$ определится как сумма их вероятностей:

$$P(\mathbf{S}_{1,a}) = P\left(\mathbf{S}_{1,a}, \overline{\theta}\right) + P\left(\mathbf{S}_{1,a}, \theta\right), \tag{1}$$

где $P\left(\mathbf{S}_{1,a}, \overline{\theta}\right)$, $P\left(\mathbf{S}_{1,a}, \theta\right)$ – вероятности аварийных событий $\left(\mathbf{S}_{1,a}, \overline{\theta}\right)$, $\left(\mathbf{S}_{1,a}, \theta\right)$ соответственно.

Вероятность аварийного события $\left(\mathbf{S}_{1,a}, \overline{\theta}\right)$ можно определить через вероятности $P(s_d)$, $P(s_a)$:

$$P\left(\mathbf{S}_{1,a}, \overline{\theta}\right) = P(s_d) \cdot \left(1 - P(s_a)\right). \tag{2}$$

Для того чтобы состоялось событие $\left(\mathbf{S}_{1,a}, \theta\right)$, должны произойти два отказа: сначала подсистемы s_a, затем подсистемы s_d. Пусть $P(s_a)^*$ – безусловная вероятность появления отказа подсистемы s_a при условии, что отказ подсистемы s_d не произойдет раньше, чем откажет s_a. Тогда [7] полная вероятность аварийного события $\left(\mathbf{S}_{1,a}, \theta\right)$:

$$P\left(\mathbf{S}_{1,a}, \theta\right) = 2 \cdot P(s_a)^* \cdot P(s_{d,\theta}). \tag{3}$$

Вероятность $P(s_a)^*$ можно определить по формуле полной вероятности. Пусть $P(s_a \cup s_d)$ – вероятность отказа подсистемы s_a либо подсистемы s_d; $P(s_a \mid s_a \cup s_d)$ – условная вероятность отказа s_a в ситуации возможного отказа подсистемы s_a либо подсистемы s_d. Тогда

$$P(s_a)^* = P(s_a \mid s_a \cup s_d) \cdot P(s_a \cup s_d). \tag{4}$$

В соответствии с теоремой Байеса для полной группы событий

$$P(s_a \mid s_a \cup s_d) = \frac{P(s_a \cup s_d \mid s_a) \cdot P(s_a)}{P(s_a \cup s_d)}, \qquad (5)$$

где $P(s_a \cup s_d \mid s_a)$ – условная вероятность события $(s_a \cup s_d)$ при отказе s_a, которая с учетом нормирования [8] для полной группы соответствующих аварийных событий определится по формуле

$$P(s_a \cup s_d \mid s_a) = \frac{P(s_a)}{P(s_a) + P(s_{d,\theta})}. \qquad (6)$$

Тогда:

$$P(s_a)^* = \frac{2 \cdot P(s_a)^2}{P(s_a) + P(s_{d,\theta})}; \qquad (7)$$

$$P(\mathbf{S}_{1,a}, \theta) = \frac{2 \cdot P(s_a)^2 \cdot P(s_{d,\theta})}{P(s_a) + P(s_{d,\theta})}. \qquad (8)$$

В результате, с учетом (1), (2), (8) получаем полную вероятность возникновения аварии в системе $\mathbf{S}_{1,a}$:

$$P(\mathbf{S}_{1,a}) = P(s_d) \cdot \big(1 - P(s_a)\big) + \frac{2 \cdot P(s_a)^2 \cdot P(s_{d,\theta})}{P(s_a) + P(s_{d,\theta})}. \qquad (9)$$

На рис. 3 приводятся результаты имитационного моделирования вероятности возникновения аварии в системе $\mathbf{S}_{1,a}$ в зависимости от изменения вероятности отказа подсистемы s_a (системы автоматического регулирования уровня воды в верховом бассейне ГАЭС). Моделирование осуществлялось при различных значениях вероятности разрушения дамбы верхового бассейна вследствие независимых от работы автоматики причин (отказа подсистемы s_d) $P(s_d)$ при условии, что в случае отказа подсистемы s_a вероятность разрушения дамбы $P(s_{d,\theta}) = 1$.

В частности, при исследованиях были промоделированы шесть случаев, когда:

1) $P(s_d) = 5 \cdot 10^{-3}$, год$^{-1}$;

2) $P(s_d) = 10^{-3}$, год$^{-1}$;

3) $P(s_d) = 5 \cdot 10^{-4}$, год$^{-1}$ (допускаемая действующими нормами [9] вероятность аварии на напорных гидросооружениях II класса);

4) $P(s_d) = 10^{-4}$, год$^{-1}$;

5) $P(s_d) = 5 \cdot 10^{-5}$, год$^{-1}$ (нормативная вероятность аварии [9] на напорных гидросооружениях I класса);

6) $P(s_d) = 10^{-5}$, год$^{-1}$.

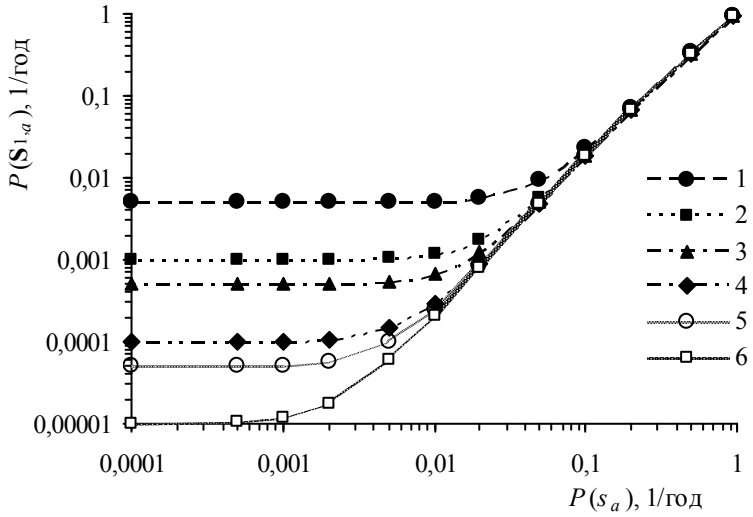

Рис. 3. Графики зависимости вероятности аварии в системе $\mathbf{S}_{1,a}$ от вероятности отказа подсистемы s_a

Анализируя графики на рис. 3, можно заметить, что во всех модельных случаях, когда вероятность отказа для системы автоматического регулирования уровня воды в верхнем бассейне ГАЭС начинает превышать некоторое «пороговое» значение, вероятность аварии в системе $\mathbf{S}_{1,a}$ начинает стремительно возрастать уже при незначительном увеличении вероятности отказа автоматики. При принятых нами вероятностях $P(s_d)$ это «пороговое» значение вероятности отказа системы автоматического регулирования меняется в пределах $10^{-3} \div 4 \cdot 10^{-2}$, год$^{-1}$. При этом при превышении «порога» для $P(s_a)$ вероятность $P(\mathbf{S}_{1,a})$ практически

перестает зависеть от вероятности первичного (независимого) отказа подсистемы s_d (т. е. собственно от надежности дамбы) и начинает зависеть главным образом от надежности автоматики.

На рис. 4 приводятся результаты имитационного моделирования вероятности системной аварии $P(\mathbf{S}_{1,a})$ в зависимости от изменения вероятности отказа подсистемы s_a при постоянном значении вероятности первичного отказа подсистемы s_d (вероятность $P(s_d) = 10^{-3}$, год$^{-1}$) и при различных значениях вероятности $P(s_{d,0})$:

1) $P(s_{d,0}) = 1$;
2) $P(s_{d,0}) = 10^{-1}$, год$^{-1}$;
3) $P(s_{d,0}) = 10^{-2}$, год$^{-1}$;
4) $P(s_{d,0}) = 10^{-3}$, год$^{-1}$;
5) $P(s_{d,0}) = 5 \cdot 10^{-4}$, год$^{-1}$;
6) $P(s_{d,0}) = 10^{-4}$, год$^{-1}$.

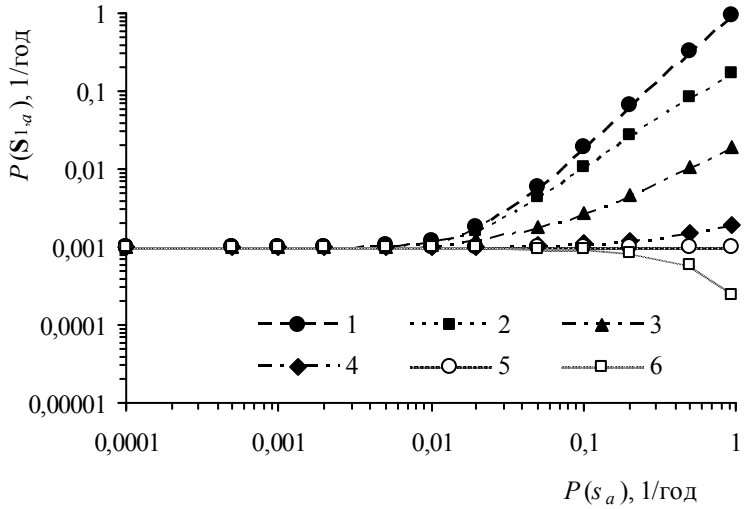

Рис. 4. Графики зависимости вероятности аварии в системе $\mathbf{S}_{1,a}$ от вероятности отказа подсистемы s_a при $P(s_d) = 10^{-3}$, год$^{-1}$

Анализируя графики на рис. 4, можно заметить, что при снижении вероятности разрушения дамбы $P(s_{d,\theta})$ при отказе подсистемы автоматического регулирования за счет работы аварийного водослива влияние отказов автоматики на вероятность $P(\mathbf{S}_{1,a})$ постепенно уменьшается.

При моделировании и оценке вероятности развития аварии на Саяно-Шушенской ГЭС рассматривалась система $\mathbf{S}_{2,a}=\{s_1, a_{1,2}, s_2\}$ в составе: агрегат ГЭС – основная подсистема (s_1); аварийный затвор – подсистема (s_2), пребывающая в «холодном» резерве; автоматический переключатель на резерв ($a_{1,2}$). При этом предполагалось, что подсистема s_2 должна «включаться» в работу автоматическим переключателем $a_{1,2}$ в случае отказа основной подсистемы s_1 и предупреждать дальнейшее развитие аварии.

Учитывались два возможные, несовместные, сценария развития аварии: сценарий A_1 – при работоспособном автоматическом переключателе на резерв отказывают как основная s_1, так и резервная s_2 подсистемы; сценарий A_2 – сначала отказывает автоматический переключатель на резерв $a_{1,2}$, а затем отказывает s_1 [10].

Несовместность сценариев A_1 и A_2 позволяет при оценке вероятности $P(\mathbf{S}_{2,a})$ развития аварии в системе $\mathbf{S}_{2,a}$ воспользоваться формулой полной вероятности. Имеем:

$$P(\mathbf{S}_{2,a}) = P(A_1) + P(A_2), \qquad (10)$$

где $P(A_1)$, $P(A_2)$ – вероятности реализации сценариев A_1 и A_2 соответственно.

Вероятность $P(A_1)$ определим при условии, что автоматический переключатель $a_{1,2}$ непосредственно при отказе подсистемы s_1, которая резервируется, пребывает в работоспособном состоянии (обозначим это условие как θ_1); вероятность $P(A_2)$ – при условии, что $a_{1,2}$ переходит в неработоспособное состояние еще при работоспособной подсистеме s_1, которая резервируется (пусть это будет условие θ_2).

Условия θ_1, θ_2, по определению, формируют полную группу событий. Поскольку сумма вероятностей условий θ_1 и θ_2 должна равняться единице, то для того чтобы задать вероятности их реализации,

достаточно определить, с какой вероятностью устройство $a_{1,2}$ откажет при работоспособной подсистеме s_1.

Для оценки вероятности отказа устройства $a_{1,2}$ при условии, что подсистема s_1 находится в работоспособном состоянии, выделим из состава системы $\mathbf{S}_{2,a}$ некоторую условную систему $\mathbf{S}_{1,a}^{ir}$, формируемую подсистемой s_1 и автоматическим переключателем на резерв $a_{1,2}$.

Предположим, что система $\mathbf{S}_{1,a}^{ir}$ (индекс ir обозначает «без резервирования») находится в работоспособном состоянии в случае, если подсистема s_1 и автоматический переключатель на резерв $a_{1,2}$ являются работоспособными, и отказывает, если откажет s_1 либо $a_{1,2}$. Пусть также между отказами подсистемы s_1 и автоматического переключателя на резерв $a_{1,2}$ отсутствуют стохастические связи, т. е. s_1 и $a_{1,2}$ отказывают вследствие собственных, независимых, внутренних, причин.

Тогда вероятность отказа устройства $a_{1,2}$ при условии, что подсистема s_1 находится в работоспособном состоянии, определится как вероятность отказа системы $\mathbf{S}_{1,a}^{ir}$ вследствие выхода из строя $a_{1,2}$.

Сформируем полную группу событий, как и в случае системных отказов A_1 и A_2, и воспользуемся формулой полной вероятности. В результате получим:

$$P(\mathbf{S}_{1,a}^{ir}) = P(\mathbf{S}_{1,a}^{ir}, s_1) + P(\mathbf{S}_{1,a}^{ir}, a_{1,2}), \tag{11}$$

где

$$P(\mathbf{S}_{1,a}^{ir}, s_1) = P(\mathbf{S}_{1,a}^{ir} \mid s_1) \cdot P(s_1), \tag{12}$$

$$P(\mathbf{S}_{1,a}^{ir}, a_{1,2}) = P(\mathbf{S}_{1,a}^{ir} \mid a_{1,2}) \cdot P(a_{1,2}). \tag{13}$$

В формулах (11)÷(13) $P(\mathbf{S}_{1,a}^{ir}, s_1)$, $P(\mathbf{S}_{1,a}^{ir}, a_{1,2})$ – безусловные вероятности, $P(\mathbf{S}_{1,a}^{ir} \mid s_1)$, $P(\mathbf{S}_{1,a}^{ir} \mid a_{1,2})$ – условные (байесовские) вероятности отказа системы $\mathbf{S}_{1,a}^{ir}$ вследствие отказов подсистемы s_1 и устройства $a_{1,2}$, соответственно.

Поскольку, по определению, для соответствующих событий-отказов справедливы отношения

$$\left(\mathbf{S}_{1,a}^{ir} \mid s_1\right) \cup \left(\mathbf{S}_{1,a}^{ir} \mid a_{1,2}\right) = \Omega,\ P(\Omega) = 1,$$

$$\left(\mathbf{S}_{1,a}^{ir} \mid s_1\right) \wedge \left(\mathbf{S}_{1,a}^{ir} \mid a_{1,2}\right) = \varnothing, \tag{14}$$

то

$$P(\mathbf{S}_{1,a}^{ir} \mid s_1) = \frac{P(s_1)}{P(s_1) + P(a_{1,2})}, \tag{15}$$

$$P(\mathbf{S}_{1,a}^{ir} \mid a_{1,2}) = \frac{P(a_{1,2})}{P(s_1) + P(a_{1,2})}. \tag{16}$$

Откуда после преобразований получим:

$$P(\mathbf{S}_{1,a}^{ir}, a_{1,2}) = \frac{P^2(a_{1,2})}{P(s_1) + P(a_{1,2})}; \tag{17}$$

$$P(\theta_2) = \frac{P^2(a_{1,2})}{P(s_1) + P(a_{1,2})}; \tag{18}$$

$$P(\theta_1) = 1 - \frac{P^2(a_{1,2})}{P(s_1) + P(a_{1,2})}; \tag{19}$$

$$P(A_1) = P(s_1) \cdot P(s_2) \cdot \left[1 - \frac{P^2(a_{1,2})}{P(s_1) + P(a_{1,2})}\right]; \tag{20}$$

$$P(A_2) = P(s_1) \cdot \frac{P^2(a_{1,2})}{P(s_1) + P(a_{1,2})}; \tag{21}$$

$$P(\mathbf{S}_{2,a}) = P(s_1) \cdot \left[P(s_2) + \frac{P^2(a_{1,2})}{P(s_1) + P(a_{1,2})}\left(1 - P(s_2)\right)\right], \tag{22}$$

где $P(s_1)$, $P(a_{1,2})$, $P(s_2)$ – вероятности отказов подсистем s_1, $a_{1,2}$, s_2 соответственно.

На рис. 5 приводятся графики зависимости вероятности развития аварии в системе $\mathbf{S}_{2,a}$ от вероятности отказа автоматического переключателя на резерв $a_{1,2}$ при различных значениях вероятности отказов под-

системы s_1 (вероятностей разрушения гидроагрегата вследствие независимых от работы автоматики причин):

1 – $P(s_1) = 10^{-1}$, год$^{-1}$;

2 – $P(s_1) = 5 \cdot 10^{-2}$, год$^{-1}$;

3 – $P(s_1) = 10^{-2}$, год$^{-1}$;

4 – $P(s_1) = 5 \cdot 10^{-3}$, год$^{-1}$;

5 – $P(s_1) = 10^{-3}$, год$^{-1}$.

Вероятность $P(s_2)$ отказа аварийно-ремонтного затвора (отказа подсистемы s_2) принималась согласно статистическим данным [11]: $P(s_2) = 10^{-2}$, год$^{-1}$.

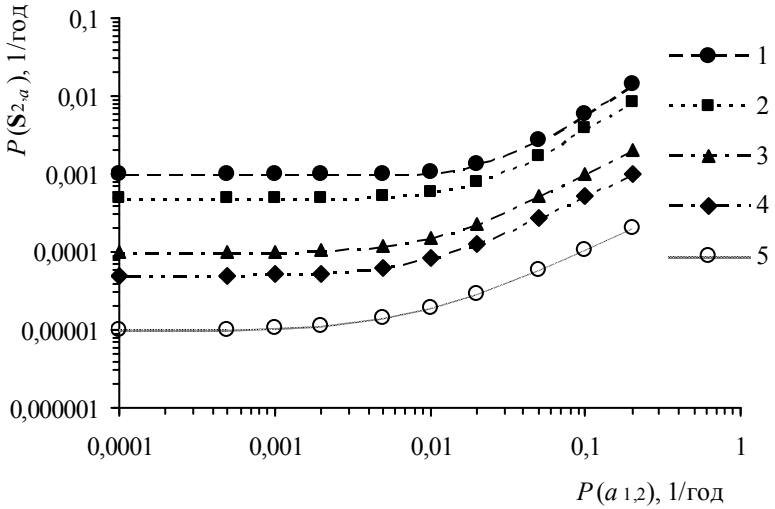

Рис. 5. Графики зависимости вероятности развития аварии в системе $\mathbf{S}_{2,a}$ от вероятности отказа автоматического переключателя на резерв $a_{1,2}$ при различных значениях вероятности разрушения гидроагрегата и $P(s_2) = 10^{-2}$, год$^{-1}$

Кроме того, дополнительно анализировалось влияние на вероятность развития аварии в системе $\mathbf{S}_{2,a}$ работоспособности аварийно-ремонтного затвора (подсистемы s_2).

На рис. 6 приводятся графики зависимости вероятности развития аварии в системе $\mathbf{S}_{2,a}$ от вероятности отказа автоматического переключателя на резерв $a_{1,2}$ при различных значениях вероятности отказа аварийно-ремонтного затвора (подсистемы s_2):

1 – $P(s_2) = 10^{-1}$, год$^{-1}$;

2 – $P(s_2) = 5 \cdot 10^{-2}$, год$^{-1}$;

3 – $P(s_2) = 10^{-2}$, год$^{-1}$;

4 – $P(s_2) = 5 \cdot 10^{-3}$, год$^{-1}$;

5 – $P(s_2) = 10^{-3}$, год$^{-1}$.

Вероятность $P(s_2)$ разрушения гидроагрегата вследствие независимых от автоматики причин (отказа подсистемы s_1) принималась равной $P(s_1) = 5 \cdot 10^{-2}$, год$^{-1}$. Эта вероятность определяет 95% надежность агрегата.

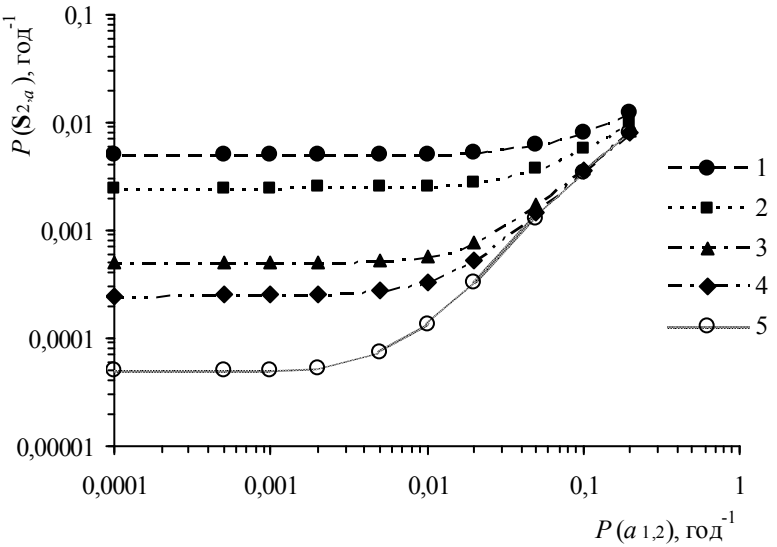

Рис. 6. Графики зависимости вероятности развития аварии в системе $\mathbf{S}_{2,a}$ от вероятности отказа автоматического переключателя на резерв $a_{1,2}$ при различных значениях вероятности отказа аварийно-ремонтного затвора и $P(s_1) = 5 \cdot 10^{-2}$, год$^{-1}$

Можно заметить, что в обоих случаях (см.рис. 5, 6) имеет место рост вероятности развития аварии в системе $\mathbf{S}_{2,a}$ при увеличении вероятности отказа автоматического переключателя на резерв $a_{1,2}$ с превышением значений, близких к 10^{-2}, год$^{-1}$. При этом отмечается высокая чувствительность вероятности развития аварии в системе к отказам автоматики в условиях, когда для обеспечения безопасности большее внимание уделяется надежности резервной подсистемы, а не основной подсистемы.

По результатам проведенных исследований можно сделать обобщающий вывод о возможности негативного влияния недостаточно надежных средств автоматического регулирования, устанавливаемых на энергетических объектах, на аварийность объектов. В то же время при обеспечении высокой работоспособности автоматики, при вероятностях отказов 10^{-3} год$^{-1}$ и ниже, можно минимизировать влияние автоматики на безопасность гидроэнергетического объекта.

Библиографический список

1. http://www.ferc.gov/industries/hydropower/safety/projects/taum-sauk/staff-rpt.asp. Taum Sauk Pumped Storage Project (No. P-2277). Dam Breach Incident. Incident Description. FERC Staff Report, April 28, 2006.
2. http://www.ferc.gov/industries/hydropower/safety/projects/taum-sauk/ipoc-rpt/full-rpt.pdf. Taum Sauk Pumped Storage Project (No. P-2277). Dam Breach Incident. Incident Description. ERC Independent Panel of Consultants (IPOC) Report, May 25, 2006.
3. http://ru.wikisource.org/wiki/ Акт технического расследования причин аварии на Саяно-Шушенской ГЭС 17 августа 2009 года. Материал из Викитеки – свободной библиотеки.
4. http://www.powermag.com/issues/features/Investigating-the-Sayano-Shushenskaya-Hydro-Power-Plant-Disaster_3229.html. Investigating the Sayano-Shushenskaya Hydro Power Plant Disaster// By A Boyko and S Popov, EKRA-Sibir Ltd. and Nemanja Krajisnik, Siemens Transmission and Distribution Ltd.
5. Брызгалов В.И. Из опыта создания и освоения Красноярской и Саяно-Шушенской гидроэлектростанций. Красноярск: Сибирский изд. дом «Суриков», 1999. – 562 с.
6. Гидротехническое строительство. НТФ «Энергопрогресс». Ежемесячный научно-технический журнал. №11. 2008.
7. Стефанишин Д.В., Романчук К.Г. Про граничні оцінки ймовірностей техногенних аварій внаслідок малоймовірних сполучень навантажень// Problems of decision making under uncertainties. Abstracts of XVI Int. Conf. Yalta, Ukraine, October 4-8, 2010. P.P. 128-129.

8. Стефанишин Д.В. Вибрані задачі оцінки ризику та прийняття рішень за умов стохастичної невизначеності. – К.: Азимут-Україна, 2009. – 104 с.
9. СНиП 33-01-2003. Гидротехнические сооружения. Основные положения. –М.: Госстрой России, 2004.
10. Стефанишин Д.В., Романчук К.Г. Оцінка ймовірності відмови зарезервованої системи з автоматичним перемиканням на резерв// Вісник НУВГП. Зб. наук. праць. Вип. 4 (44). Рівне: НУВГП. 2008. С. 334-340.
11. Lagerholm S. Safety and reliability of spillway gates// Repair and upgrading of dams Symposium. -Stockholm: 1996. -P. P. 362-373.