УДК 004.832.2

М.А. ЯСТРЕБЕНЕЦКИЙ, В.В. ИНЮШЕВ, О.Н. БУТОВА

Государственный научно-технический центр по ядерной и радиационной безопасности, Украина

ОЦЕНКА УРОВНЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АЭС

Определены количественные значения показателей безопасности информационных и управляющих систем АЭС для различных категорий нарушений безопасности

АЭС, безопасность, информационные и управляющие системы

Выявление особенностей ИУС АЭС

Поскольку некоторые положения работы могут быть применены не только для информационных и управляющих систем (ИУС) АЭС, но и для ИУС иных критических объектов, предпошлем изложению результатов выявление особенностей ИУС АЭС. Ряд таких особенностей являются общими для любых систем АЭС, не только ИУС. К ним относятся:

1) наличие государственного органа, целью которого является обеспечение (регулирование) ядерной и радиационной безопасности. Этот орган принципиально независим как от АЭС, иных организаций, использующих атомную энергию, так и от иных органов власти и, конечно, от разработчиков или проектировщиков АЭС. Такие органы регулирования согласно Конвенции о ядерной безопасности [1] имеются во всех странах, где есть АЭС, включая Украину (Государственный комитет ядерного регулирования – Держатомрегулювання);

2) принятие принципа «запрещено то, что не разрешено» в отличие от принятого в ряде отраслей техники и общественной деятельности принципа «разрешено то, что не запрещено»;

3) обязательность независимой государственной экспертизы, целью которой являются исследование, проверка и оценка соответствия объекта экспертизы требованиям ядерной и радиационной безопасности с целью подготовки обоснованного заключения для принятия решения Держатомрегулюванням. Объектом экспертизы в нашем случае являются ИУС, включая их компоненты (технические средства, программное обеспечение, программно-технические комплексы);

4) обязательная классификация всех систем и их элементов (включая ИУС) в зависимости от влияния на безопасность, где выделяются системы, важные для безопасности (safety important systems), которые делятся на несколько классов (категорий). К сожалению, классификация по безопасности ИУС АЭС, действующая в Украине [2], не отражает современные изменения в международной классификации, принятые затем и в ряде национальных документов (эти отличия рассматривались в [3]);

5) наличие влиятельной международной организации – МАГАТЭ, занимающейся в международном масштабе разными проблемами использования ядерной энергии, но, пожалуй, в первую очередь – безопасностью АЭС, включая вопросы, касающиеся ИУС АЭС;

6) наличие большого числа международных нормативных документов (МАГАТЭ, МЭК) по безопасности АЭС, ряд из которых посвящен ИУС АЭС (например [4 – 6]);

7) открытость работ по безопасности, наличие разнообразных проверок международными организациями, независимого партнерского анализа (peer review), гарантированный доступ к опыту других стран.

Некоторые аспекты сопоставления ИУС АЭС и ИУС в других критических отраслях техники при-

ведены в статьях [7] (ИУС АЭС и системы управления ракетами-носителями), и [8] (ИУС АЭС и системы управления ракетно-космическими комплексами). В дополнение к этим работам укажем, что для ИУС АЭС доля нарушений безопасности по вине программного обеспечения меньше, чем в ракетно-космической технике. Это, может объясняться возможностью вмешательства оперативного персонала в управление энергоблоком при отказах программного обеспечения.

Безопасность ИУС АЭС

Ситуация с безопасностью ИУС АЭС в настоящее время в определенной степени аналогична ситуации с надежностью ИУС промышленных объектов, включая АЭС, имевшей место в шестидесятые годы. Приведем примеры:

1. Надежность (ранее): шли дискуссии о терминологии, начиная с базового определения понятия «надежность».

Безопасность (сейчас): отсутствует согласованное и непротиворечивое определение понятия «безопасность». Отметим, что безопасность является свойством, как и надежность. В то же время в Законе Украины, посвященном ядерной безопасности [9] и нормативном документе Украины [2] под ядерной и радиационной безопасностью понимается процесс (соблюдение). В некоторых международных документах безопасность определяется как состояние и т.д.

2. Надежность (ранее): не вызывала сомнений необходимость обеспечения надежности, но далеко не все считали нужным оценку количественных значений показателей надежности – спрашивая: «А что мы будем делать с Вашими цифрами».

Безопасность (сейчас): зачем нужны количественные значения показателей безопасности, в частности применительно к ИУС АЭС.

3. Надежность (ранее): показатели надежности отсутствовали в технических заданиях (ТЗ) на разработку ИУС, методы оценки надежности ИУС по результатам эксплуатации только начали разрабатываться*. Безопасность (сейчас): не решен вопрос, каковы количественные показатели безопасности ИУС АЭС, нужно ли их задавать в ТЗ и вообще, зачем они нужны.

Функциональная безопасность ИУС

Стандарт МЭК 61508 [12] посвящен функциональной безопасности электрических/электронных/программируемых электронных (Э/Э/ПЭ) систем.

Понятие *функциональная безопасность ИУС* относится к совокупности управляемого оборудования и системы управления этим оборудованием и определяется как часть общей безопасности, которая зависит от правильного функционирования Э/Э/ПЭ с другими технологическими системами, а также внешними устройствами для снижения риска.

Следуя [12], *функциональной безопасностью ИУС АЭС* можно назвать часть свойства “безопасность АЭС”, которая относится к совместно функционирующим ИУС и технологическому оборудованию и зависит от правильного функционирования ИУС.

Подобно тому, как оценке надежности систем предшествует формализация понятия ее отказ, оценке функциональной безопасности системы следует предшествовать определению того, что понимается под нарушением безопасности и как их классифицировать.

Для АЭС определение и классификация ядерных событий описаны в ряде нормативных документов:

– международном МАГАТЭ, где имеется шкала INES (International Nuclear Event Scale) [13];

– нормах и правилах по ядерной безопасности Украины [14].

Нарушения разделяются на аварии и происшествия (инциденты). Методы оценки функциональной безопасности различны в зависимости от категории нарушений.

---

*В связи с этим отметим, что когда много лет назад мы, по-видимому, впервые в СССР определили значения показателей надежности автоматических систем тепловых электростанций (см. [10, 11]) у ряда людей возникал вопрос – а что вы будете делать с этими показателями, зачем они нужны.

a) ***Аварии***.

Показатели безопасности энергоблока АЭС для аварий задаются в «Общих положениях» [2].

Вероятность предельного аварийного выброса за определенное время для проектируемых блоков не должна превышать 10^{-6} реактор/год, а для действующих и строящихся блоков - 10^{-5} реактор/год. Такой выброс классифицируется уровнем 6 и 7 по INES [13] и категориям А01 и А02 по [14].

Вероятность тяжелого повреждения активной зоны за определенное время Р должна быть ниже 10^{-4} реактор/год для действующих и строящихся блоков, 10^{-5} реактор/год для вновь проектируемых блоков. Такие повреждения классифицируются уровнем 4 по INES [13] и категориями А03, А04 по [14].

Аналитическая оценка этих показателей проводится в рамках вероятностного анализа безопасности (ВАБ), где ВАБ 1-го уровня (ВАБ-1) оценивает частоту повреждения активной зоны, ВАБ 2-го уровня (ВАБ-2) - частоту сверхнормативных выбросов. ВАБ начала проводиться в СССР после аварии на ЧАЭС (см., например, [15]) и в настоящее время выполняется для всех энергоблоков АЭС Украины.

Показателем функциональной безопасности по авариям назовем вероятность отсутствия аварии по вине отдельных ИУС или всей системы управления технологическим процессом энергоблока (СУТПЭ). Для СУТПЭ этот показатель

$$P_{СУТПЭ} = P \cdot \alpha.,$$

где α. – доля нарушений, вызываемых СУТПЭ.

Определение α. является одной из задач ВАБ и представляет несомненный интерес. К настоящему времени эти величины, по-видимому, не определялись.

Ниже ограничимся только оценкой величины Р. За время существования промышленных АЭС в мире предельный аварийный выброс, соответствующий уровню 7 INES, имел место только при аварии на ЧАЭС в 1986 г. Тяжелое повреждение активной зоны, соответствующее уровню 4, имело место на энергоблоке «Три-Майл-Айленд» в 1979 г.

За все время эксплуатации АЭС с реакторами ВВЭР аварий не было: суммарная наработка АЭС с этими реакторами в Украине, начиная с пуска в 1980 г. энергоблока №1 Ровенской АЭС, к началу 2007 г. составила 270 реакторолет (совместно ВВЭР-1000 и ВВЭР-440). Суммарная наработка всех АЭС различных стран с этими реакторами, включая реакторы, выведенные из эксплуатации, составила 1220 реакторолет.

Отсюда можно определить верхнюю доверительную границу вероятности повреждения активной зоны реакторов типа ВВЭР с доверительной вероятностью 0,9. Эта величина составляет:

- для реакторов Украины Р = $8{,}6 \cdot 10^{-3}$ реактор/год;

- для всех реакторов типа ВВЭР = $1{,}9 \cdot 10^{-3}$ реактор/год.

Указанные величины приведены не для доказательства справедливости показателя, заданного в [5], – такое доказательство невозможно, учитывая реальное число имеющихся и строящихся реакторов ВВЭР. Однако эти цифры в некоторой степени иллюстрируют статистически подтвержденный уровень безопасности АЭС.

b) ***Происшествия (инциденты).***

Методы оценки показателей функциональной безопасности ИУС классифицируем по двум признакам:

- в зависимости от способа оценок:
  - расчетный;
  - статистический;

- в зависимости от необходимости рассмотрения управляемого технологического оборудования:
  - анализ замкнутого контура "ИУС – объект управления";
  - анализ только ИУС без учета объекта управления.

Аналитические методы оценки функциональной безопасности ИУС без учета объекта управления пригодны для категорий нарушений, характеризующихся неработоспособностью систем безопасности или каналов безопасности (категории П03, П04, П05, П07, П09, П10 согласно [14]). Методы оценки следуют из теории надежности (например, [16 – 18]).

Аналитические методы оценки функциональной безопасности с учетом объекта управления для иных категорий происшествий до настоящего времени не развивались.

Статистические методы могут быть применены для оценки функциональной безопасности по различным категориям происшествий.

Результаты статистической оценки

Приведем сначала некоторые результаты статистической оценки безопасности энергоблоков ВВЭР-1000 и ВВЭР-440 по всем категориям нарушений безопасности и из-за всех причин, полученные за 1996-2005гг. на основании общей базы данных о нарушениях в работе АЭС, имеющейся в ГНТЦ ЯРБ. Аварий за это время не было. Суммарное число рассмотренных нарушений - 528.

График интенсивности потока нарушений (для всех блоков ВВЭР-1000) в зависимости от времени дан на рис. 1, для энергоблоков ВВЭР-440 – на рис. 2 (см. также результаты анализа изменения числа нарушений во времени, приведенные в [19]).

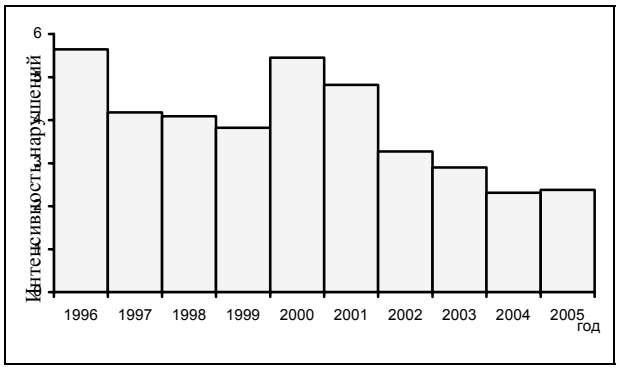

Рис. 1. График интенсивности потока нарушений в работе блоков ВВЭР-1000 АЭС Украины в зависимости от календарного времени

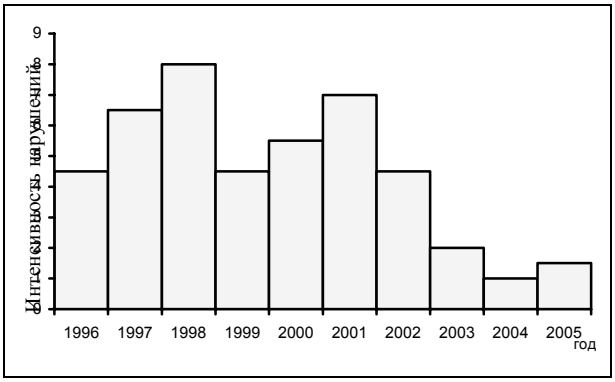

Рис. 2. График интенсивности потока нарушений в работе блоков ВВЭР-440 АЭС Украины в зависимости от календарного времени

График интенсивности потока нарушений АЭС для всех блоков ВВЭР-1000 в зависимости от возраста блоков дан на рис. 3, для энергоблоков ВВЭР-440 – на рис. 4.

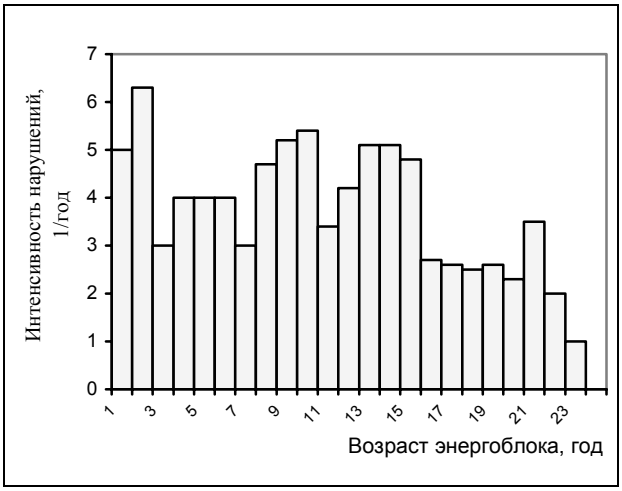

Рис. 3. График интенсивности потока нарушений в работе блоков ВВЭР-1000 АЭС Украины в зависимости от возраста

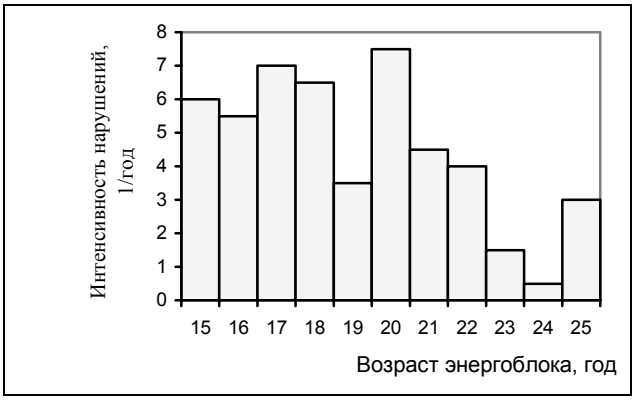

Рис. 4. График интенсивности потока нарушений в работе блоков ВВЭР-440 АЭС Украины в зависимости от возраста

Как следует из этих рисунков, имеет место снижение интенсивности потока нарушений во времени, что объясняется улучшением качества эксплуатации и проводимой модернизацией оборудования.

Отметим, что повышение безопасности АЭС в календарном времени отражает общую тенденцию постепенного повышения безопасности различных критических объектов (см., например, [20] для катастроф в гражданской авиации).

Вероятности нарушений различных категорий приведены в табл. 1, условные вероятности нарушения $i^{й}$ категории при условии, что предыдущее нарушение было $j^{й}$ категории, даны в табл. 2.

Гистограмма распределения времени между нарушениями (безотносительно категории) приведена на рис. 5. Это распределение достаточно хорошо совпадает с экспоненциальным.

Таблица 1

Вероятность нарушений различных категорий в работе энергоблоков ВВЭР-1000 АЭС Украины

Категория нарушений	П01	П02	П03	П04	П05	П06	П07	П08	П09	П10
Вероятность	0,005	0,04	0,005	0,002	0,4	0,016	0,19	0,176	0036	0,13

Таблица 2

Условная вероятность нарушений i-й категории при условии, что предыдущее нарушение было j-й категории в работе энергоблоков ВВЭР-1000 АЭС Украины

		Категория j									
		П01	П02	П03	П04	П05	П06	П07	П08	П09	П10
Условная вероятность нарушений i-ой категории	П01	0	0	0	0	0	0,5	0	0	0	0,5
	П02	0	0,056	0	0	0,389	0	0,167	0,111	0,056	0,222
	П03	0	0	0	0	0,5	0	0	0	0	0,5
	П04	0	0	0	0	0	0	0	1	0	0
	П05	0,006	0,03	0	0	0,518	0,006	0,137	0,167	0,03	0,107
	П06	0	0,143	0	0,143	0,286	0	0,143	0,143	0	0,143
	П07	0	0,063	0	0	0,338	0,025	0,325	0,138	0,05	0,063
	П08	0,014	0,027	0	0	0,365	0,041	0,189	0,284	0,0136	0,068
	П09	0	0,063	0	0	0,25	0	0,375	0,125	0,063	0,125
	П10	0	0,035	0,035	0	0,246	0	0,175	0,14	0,07	0,299

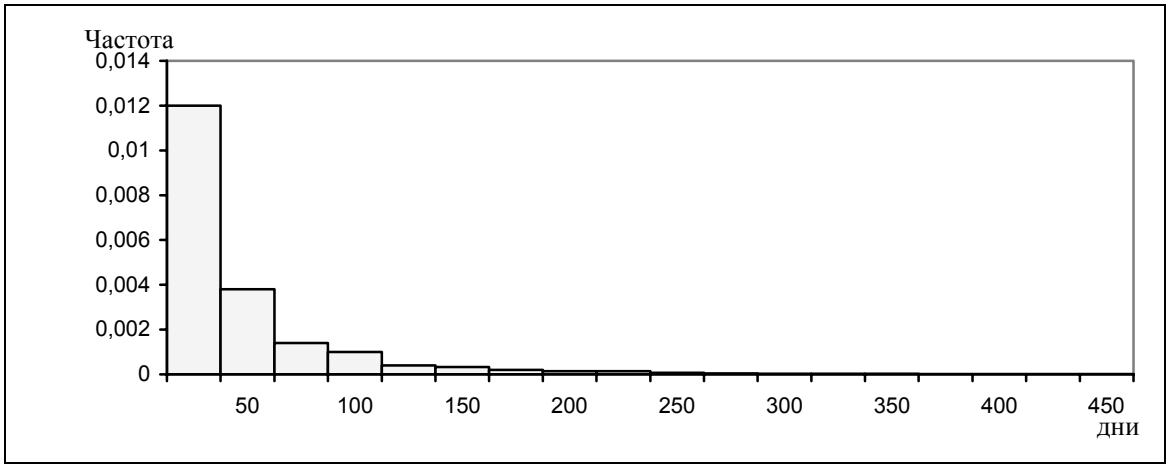

Рис. 5. Гистограмма распределения времени между нарушениями в работе энергоблоков ВВЭР-1000

5. Средняя доля нарушений из-за ИУС за рассмотренное время составила 21,2 %.

Отметим, что по данным России за 1992-2003 гг. (см. [21]), эта доля, средняя для блоков ВВЭР и РБМК, составила 20,6 %. Оценка показателей функциональной безопасности СУТПЭ за 1996-2005 годы по различным видам нарушений даны в табл. 3.

Таблица 3

Результаты статической оценки показателей функциональной безопасности ИУС

Вид нарушения	Категория нарушения	ВВЭР-1000			ВВЭР-440		
		Кол-во нарушений	Параметр потока нарушений	Вероятность отсутствия нарушения за 1 год	Кол-во нарушений	Параметр потока нарушений	Вероятность отсутствия нарушения за 1 год
Авария	А01-А04	0	-	-	0	-	-
Происшествия	П01	0	-	-	0	-	-
	П02	5	0,04	0,961	0	-	-
	П03	2	0,02	0,98	0	-	-
	П04	1	0,009	0,991	0	-	-
	П05	42	0,37	0,691	5	0,25	0,779
	П06	0	-	-	0	-	-
	П07	22	0,19	0,827	4	0,2	0,819
	П08	17	0,15	0,861	5	0,25	0,779
	П09	3	0,03	0,97	1	0,05	0,951
	П10	5	0,04	0,961	0	-	-
Общее количество нарушений		**97**	**0,85**	**0,427**	**15**	**0,75**	**0,472**

График зависимости интенсивности потока нарушений, вызванных неправильным функционированием СУТПЭ, в зависимости от календарного времени дан на рис. 6 для блоков ВВЭР-1000 и рис. 7 для блоков ВВЭР-440.

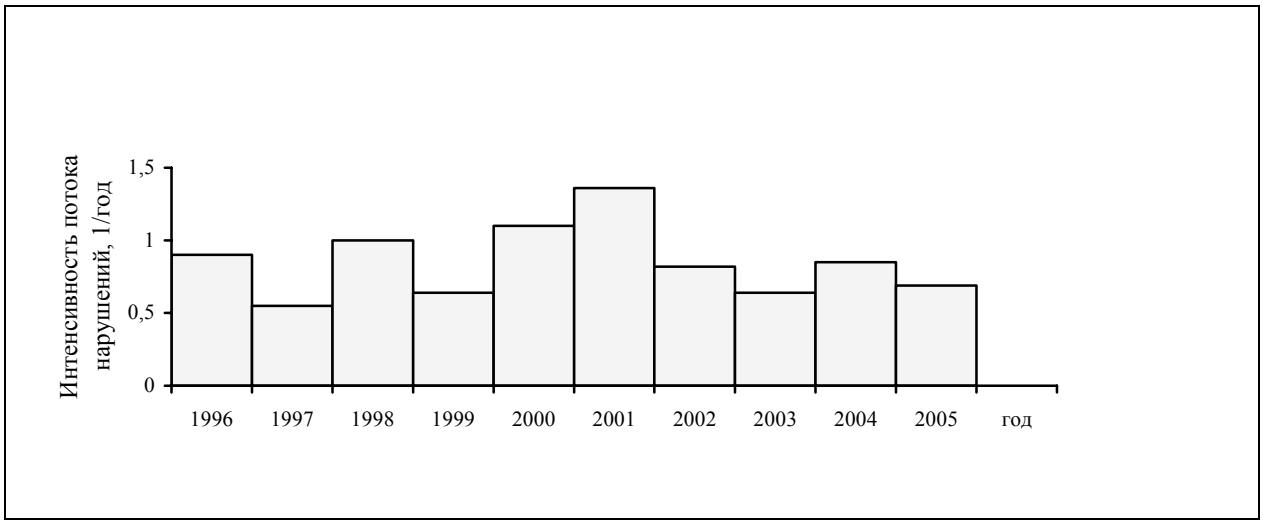

Рис. 6. График интенсивности потока нарушений, вызванных неправильным функционированием ИУС в работе блоков ВВЭР-1000 АЭС Украины, от календарного времени

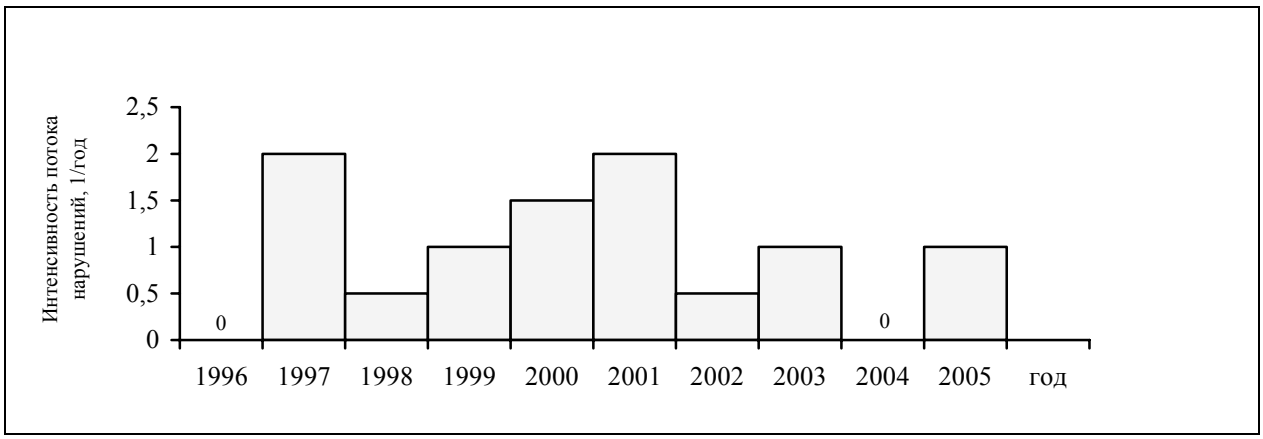

Рис. 7. График интенсивности потока нарушений, вызванных неправильным функционированием ИУС в работе блоков ВВЭР-440 АЭС Украины, от календарного времени

Графики зависимости интенсивности потока нарушений, вызванных неправильным функционированием СУТПЭ, в зависимости от возраста блока даны на рис. 8 для блоков ВВЭР-1000 и рис. 9 для блоков ВВЭР-440. Полученные результаты использованы для выработки стратегии модернизации оборудования АЭС.

Эти данные являются продолжением ранее полученных результатов, опубликованных в [22].

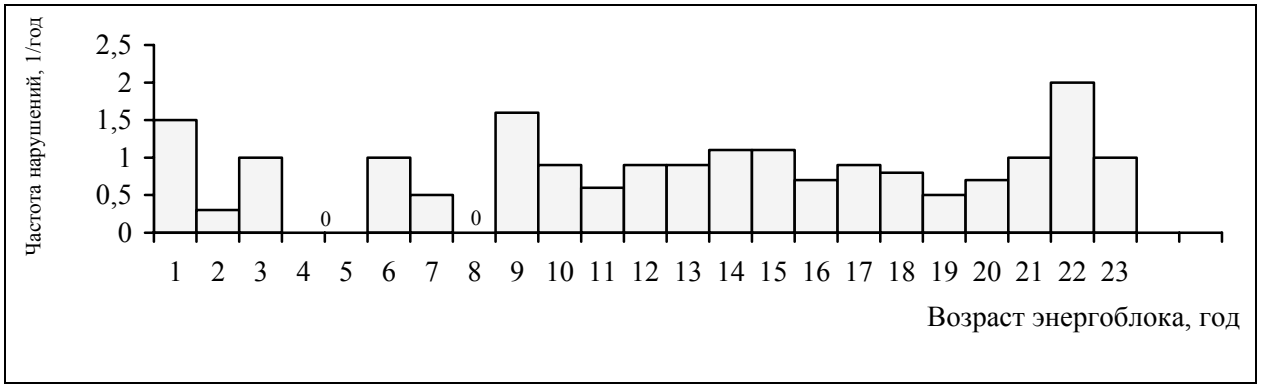

Рис. 8. График интенсивности потока нарушений, вызванных неправильным функционированием ИУС в работе блоков ВВЭР-1000 АЭС Украины, от возраста

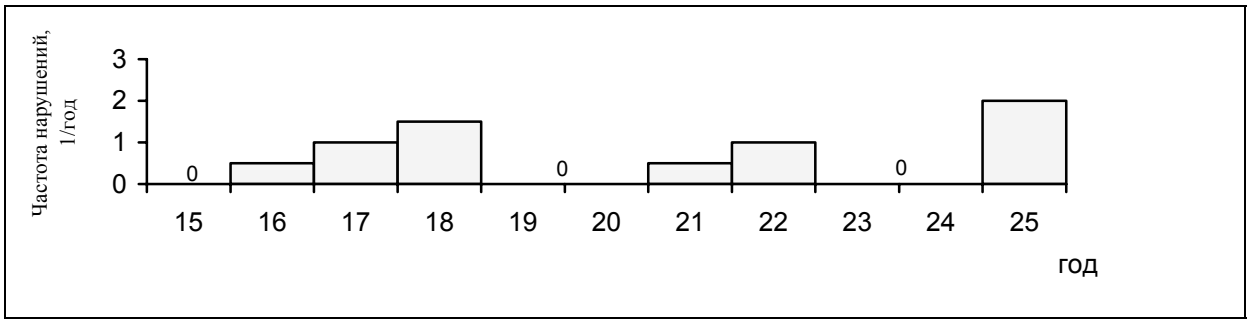

Рис. 9. График интенсивности потока нарушений, вызванных неправильным функционированием ИУС в работе блоков ВВЭР-440 АЭС Украины, от возраста

Литература

1. Конвенція про ядерну безпеку // Ядерне законодавство. – К.: Видавничий дім, 1999. – Т.2.

2. Общие положения обеспечения безопасности атомных станций, НП 306.1.02/1.034-2000. К.: Государственная Администрация ядерного регулирования, 2000.

3. Ястребенецкий М.А., Розен Ю.В. О классификации по безопасности информационных и управляющих систем и их компонентов // Ядерная и радиационная безопасность. – 2004. – № 4. – С. 35-41.

4. IAEA NS-G-1.1. Software for computer based systems important to safety in nuclear power plants. Safety guide. Vienna, 2000.

5. IAEA NS-G-1.1. Software for computer based systems important to safety in nuclear power plants. Safety guide. Vienna, 2000.

6. IEC 61513. Nuclear power plants - instrumentation and control for systems important to safety – general requirements for systems.

7. Айзенберг А.Е., Ястребенецкий М.А. Сопоставление принципов обеспечения безопасности систем управления ракетами-носителями и атомными электростанциями // Космічна наука і технология. – 2002. – № 1. – С. 21-23.

8. Скляр В.В., Харченко В.С., Ястребенецкий М.А. Цифровые информационные и управляющие системы атомных электростанций и ракетно-космических комплексов: сравнительный анализ, тенденции развития, обеспечение безопасности // Ядерная и радиационная безопасность. – 2004. – № 2. – С. 51-57.

9. Закон Украины «Об использовании ядерной энергии и радиационной безопасности». №39/95-ВР от 08.02.95.

10. Соляник Б.Л., Комаров Г.П., Ястребенецкий М.А. Определение надёжности автоматических регуляторов в условиях эксплуатации на тепловой электростанции // Теплоэнергетика. – 1965. – № 4. – С. 27-31.

11. Ястребенецкий М.А., Соляник Б.Л., Комаров Г.П. Характеристики ремонтопригодности аппаратуры автоматики тепловой электростанции // Теплоэнергетика. – 1966. – № 9. – С. 9-14.

12. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety/related systems.

13. IAEA/OECD/NEA. The International Nuclear Event Scale. User's manual. 2001 Edition, IAEA, Vienna, 2001.

14. НП 306.2.100-2004. Положение о порядке расследования и учета нарушений в работе атомных электрических станций. – К., 2005.

15. Швыряев Ю.В. и др. Вероятностный анализ безопасности атомных станций. Методика выполнения. – М.: ИАЭ им. И.В.Курчатова, 1992. – 124 с.

16. Дружинин Г.В. Надежность автоматизированных производственных систем. – М.: Энергоатомиздат. – 256 с.

17. Глазунов Л.П., Грабовецкий В.П., Щербаков О.В. Основы теории надежности автоматических систем управления. – Л.: Энергоатомиздат, 1984. – 456 с.

18. Ястребенецкий М.А., Иванова Г.М. Надежность автоматизированных систем управления технологическими процессами. – М.: Энергоатомиздат, 1989. – 166 с.

19. Лігоцький О.І., Недбай С.В., Носовський А.В. Аналіз потоку порушень в роботі АЕС України, які сталися протягом 2005 року // Ядерная и радиационная безопасность. – 2004. – № 3. – С. 55-61.

20. Безпека авіації / За ред. В.П. Бабака. – К.: Техніка, 2004. – 240 с.

21. Кузнецов В.М. Эффективность формирования обеспечения и поддержания надежности. Современное состояние безопасности объектов использования атомной энергетики // Надежность. – 2006. – № 3. – С. 11-18.

22. Ястребенецкий М.А., Бутова О.Н., Инюшев В.В., Спектор Л.Л. Показатели функциональной безопасности систем управления энергоблоком АЭС // Ядерные измерительно-информационные технологии. – 2005. – № 3. – С. 35-40.

Поступила в редакцию 12.03.2007

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.