PolotskSU

**Парламентское собрание Союза Беларуси и России**

**Постоянный Комитет Союзного государства**

**Оперативно-аналитический центр**
**при Президенте Республики Беларусь**

**Государственное предприятие «НИИ ТЗИ»**

**Полоцкий государственный университет**

# КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

PolotskSU

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

**УДК 004(470+476)(061.3)**
**ББК 32.81(4Беи+2)**

**ISBN 978-985-531-564-4**

© Полоцкий государственный университет», 2017

PolotskSU



4. Севбо И.П. Структура связного текста и автоматизация реферирования / М.: Наука, 1969, 135с.

5. Jurafsky D. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition / D. Jurafsky, J.H. Martin. – New Jersey: Prentice Hall, 2000, 934p.

# О ФОРМИРОВАНИИ ЦЕНТРАЛИЗОВАННОГО АУДИТА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОСТАВЕ ПОДСИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ РЕСПУБЛИКИ БЕЛАРУСЬ

А.О. МОЛЧАН, О.Э. СЯЗАНЦЕВ, Н.В. ЖУРАВСКИЙ

*Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»*

В силу быстро растущей информатизации общества количество хранимой, обрабатываемой и передаваемой в электронном виде информации растет в геометрической прогрессии. Как следствие, все в большем масштабе поднимается проблема общедоступности информации, а также взаимодействия с информацией, распространение и (или) представление которой ограничено. Возникает острая необходимость в контроле и ограничении доступа к обрабатываемой информации, а также в своевременной информированности ответственных за информационную безопасность (далее – ИБ) лиц об инцидентах ИБ. Помимо общедоступности информации уязвимость информационных систем (ИС) возрастает также за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема программного обеспечения (ПО).

Для мониторинга ИС на предмет корректного функционирования всех ее процессов, активов и ресурсов, а также сохранности информации, доступ к которой ограничен, в составе системы защиты информации (СЗИ) ИС организуется подсистема аудита событий ИБ.

Системы аудита событий ИБ используются для мониторинга ИС на предмет корректного функционирования и сохранности информации, доступ к которой ограничен. На данный момент существует множество средств аудита событий ИБ, как встроенных в общесистемное ПО, так и специально разработанных программных и программно-аппаратные комплексов компаниями и корпорациями разных стран. Однако в государственных ИС согласно законодательству Республики Беларусь в области защиты информации (ЗИ) допустимо использование только тех средств ЗИ, которые прошли сертификацию по требованиям безопасности информации и получили сертификат соответствия либо экспертное заключение на соответствие требованиям технических нормативных правовых актов в области технического нормирования и стандартизации.

Многие средства ЗИ ведут журналы аудита автономно, и интеграция их производится вручную ответственными за ИБ лицами. Главная проблема формирования централизованного аудита ИБ в составе СЗИ ИС на данный момент является дороговизна иностранных продуктов (в частности, систем SIEM) и ограниченное представление систем аудита ИБ белорусского производства на рынке средств ЗИ, которые также позволяли бы снизить угрозы ИБ.

PolotskSU



Для решения данного вопроса были выявлены требования к подсистеме аудита ИБ на основании законодательной базы Республики Беларусь, обеспечивающие максимальную безопасность в современных условиях, проведен анализ средств аудита ИБ представленных в реестре средств ЗИ, утвержденном Оперативно-аналитическим центром при Президенте Республики Беларусь, сформулированы рекомендации по формированию централизованного аудита ИБ.

# МОНИТОРИНГ ВИБРОСОСТОЯНИЯ ТУРБОГЕНЕРАТОРОВ ТЭЦ С ПОМОЩЬЮ ГЛУБИННЫХ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Р.Н. МЯСОУТОВ, Д.А. АКИМОВ

*Московский технологический университет*

В настоящее время в России находится в эксплуатации большое количество паровых турбоагрегатов [1]. В основном это паровые турбоагрегаты в схемах паросилового оборудования различной мощности. Кроме того, в 2000 годах введен в эксплуатацию ряд паровых турбоагрегатов в составе парогазовых энергоблоков. В современных условиях турбогенераторы зачастую работают на предельных режимах, и их эксплуатация требует особого отношения к контролю режимов работы и диагностике состояния машины. Турбогенераторы отличаются большими продольными размерами, значительной сложностью конструкции, а возникший в одном из элементов конструкции дефект, вызывающий повышение уровня вибраций, оказывает непосредственное влияние на сопряженные с ним другие элементы турбогенератора. В связи с этим в последнее время особый интерес проявляется к созданию систем мониторинга и вибродиагностики, которые не только обеспечивают выявление повышенной виброактивности машины, но и на основе результатов анализа полученной виброинформации позволяют выявлять причины возникновения такой виброактивности, а также сформулировать технические решения и рекомендации по её устранению. Мониторинг технического состояния турбоагрегата – это наблюдение за процессом изменения его работоспособности с целью предупреждения персонала о достижении предельного состояния, что позволяет перевести большинство отказов из категории внезапных для персонала в категорию постепенных за счет раннего их обнаружения и своевременного предупреждения [2, 3]. Мониторинг машин с помощью таких систем проводится в режиме реального времени и необходим для непрерывного наблюдения за вибросостоянием машины, в частности, за уровнем вибраций ее основных узлов и элементов. Диагностика дефектов выполняется на основе заранее сформированных экспериментальных баз данных и обобщенных баз знаний, ставящих в соответствие повышенный уровень виброактивности с вызвавшими ее причинами.

При применении методов обнаружения неисправностей на основе математических моделей следует различать конфигурации объектов. Что касается внутренних связей, используемых при обнаружении неисправностей, и возможностей различать неисправности, ситуация существенно улучшается из-за доступности дополнительных измерений.

Для формирования пространства признаков при нейросетевой классификации необходимо определить требования к признакам основных видов неисправностей турбогенераторов ТЭС.