Министерство науки и высшего образования Российской Федерации

Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 Информационная безопасность

ФГАОУ ВО «Северо-Кавказский федеральный университет»

СБОРНИК ДОКЛАДОВ XXIII ПЛЕНУМА ФУМО ВО ИБ И ВСЕРОССИЙСКОЙ НАУЧНОЙ КОНФЕРЕНЦИИ «ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ» (ИНФОБЕЗОПАСНОСТЬ –2019)

Ставрополь

2019

УДК 004.45
ББК 32.972.5
С23

С23 **Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ –2019)** / Отв. редактор: В.И. Петренко; Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 Информационная безопасность ФГАОУ ВО «Северо-Кавказский федеральный университет»; ФГАОУ ВО «СевероКавказский федеральный университет». – Ставрополь: Изд-во СКФУ, 2019. – 300 с.

Настоящий сборник содержит доклады XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации»

УДК 004.45
ББК 32.972.5

Спонсоры конференции:

ООО **«Открытая мобильная платформа»**
ООО **«РусБИТех-Астра»**
ООО **«Монтажно-технологическое управление «Телеком-С»**
ООО **«АЛЬФА»**

Содержание

СЕКЦИЯ 1. «ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ»

Концепция мониторинга целостности телеметрической информации о состоянии энергетической установки летательного аппарата

А.И. Фрид
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: frid46@mail.ru

М.Б. Гузаиров
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: guzairov@ugatu.su

А.М. Вульфин
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: vulfin.alexey@gmail.com

В.В. Берхольц
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: torina4@yandex.ru

Аннотация

Рассмотрены вопросы создания системы мониторинга целостности накапливаемых данных в модульной системе сбора, хранения и обработки телеметрической информации о состоянии энергетической установки летательного аппарата на основе применения ее модели и современных технологий интеллектуального анализа телеметрической информации.

Ключевые слова: система сбора, хранения и обработки телеметрической информации, автоматизированная информационная система, целостность данных измерений, модель энергетической установки.

1. Введение

В настоящее время эксплуатируется и разрабатывается множество типов энергетических установок (ЭУ) летательного аппарата (ЛА): газотурбинные, электрические, на ядерном топливе, ракетные двигатели и т.д. Повышение эффективности обслуживания ЭУ ЛА возможно, в частности, за счет снижения времени, затрачиваемого на контроль и диагностику его технического состояния, что требует использования оперативных и эффективных методов контроля на основе комплексной автоматизации и интеллектуализации. Эффективность контроля состояния ЭУ существенно зависит от вероятности корректного определения его технического состояния, что определяет экономичность и безопасность полетов [1, 2].

Развитие технологий контроля параметров ЭУ связано с совершенствованием алгоритмического и математического обеспечения информационных систем, позволяющего учитывать нестационарность физических процессов при эксплуатации, сложность их математического описания, зависимость технических характеристик от внешних условий работы, ограниченный состав измеряемых параметров, их технологический разброс и т. д. [1, 2].

Цифровые системы управления ЭУ содержат встроенные системы контроля и диагностики

«1», с множеством элементов облика S_j, изначально не подлежащих защите (при этом, если мера включения на 5-м шаге получилась равной меньше «1», то делается вывод, что элементы облика S_j не подлежат защите):

$$C_{сх}\left(S_j^{защ}, S_j\right) = \frac{2card\left(S_j^{защ} \cap S_j\right)}{card\left(S_j^{защ}\right) + card\left(S_j\right)}, \quad \forall S_j^{защ} \left| W_{вкл}\left(S_j^{защ}, B\right) = 1. \right. \tag{6}$$

На седьмом шаге по максимуму значения меры сходства определяются элементы облика ОВТ изначально не отнесенные к защищаемым, которые подлежат защите:

$$S_j^* = S_j \left| C_{сх}\left(S_j^{защ}, S_j\right) = \max_{S_j \in S} C_{сх}\left(S_j^{защ}, S_j\right). \right. \tag{7}$$

На восьмом шаге полученные элементы облика S_j^*, исключаются из матрицы совокупного объема сведений B и осуществляется выполнение шага 5 (определение меры включения $W_{вкл}$ элементов облика $S_j^{защ}$ в полученное множество матрицы B совокупного объема свойств элементов облика ОВТ, не подлежащих защите). При этом значение пятого шага $W_{вкл}\left(S_j^{защ}, B\right) < 1$ завершает последовательность действий и формируются полученные искомые элементы облика S_j^*, подлежащие защите.

4. Результаты

Результатом работы является методика, основывающаяся на методе морфологического анализа и позволяющая с учетом семантических связей облика ОВТ решить актуальную задачу по определению его ОС.

На основе предложенной методики разработана «Программа определения защищаемых элементов изделия» [7].

5. Заключение

В данной статье представлена методика определения охраняемых сведений об образце военной техники, основывающаяся на методе морфологического анализа и учитывающая семантические связи между элементами облика ОВТ. Применение данной методики для определения охраняемых сведений об образце военной техники позволяет снизить субъективность экспертных оценок.

Список используемых источников

1. Федеральный Закон Российской Федерации от 21 июля 1993 года № 5485-1 "О государственной тайне" // Собрание законодательства РФ. – 1997 – № 41. – С. 8220-8235
2. Модель облика образца вооружения и военной техники на этапах жизненного цикла изделия / А.В. Радионов, В.А. Мельник // Научно-практический междисциплинарный журнал «Стратегическая стабильность», выпуск №4 (85), 2018г., с. 61 – 63
3. Исследовательский Центр Виктора Воксанаева [Электронный ресурс]: Информационный бюллетень OSINT № 33 (октябрь 2013 г.). – URL: http://viktorvoksanaev.narod.ru/voksanaev.html/ (дата обращения: 08.09.2019)
4. Анализ информационных процессов на этапах жизненного цикла образцов вооружения и военной техники / А.В. Радионов // Труды 4ЦНИИ Минобороны России. Материалы Всероссийской научно-технической конференции «Создание и развитие средств защиты информации и информационного противоборства в РВСН» – 2018 – вып. №142, т.1, ч.1 – С.134-136
5. Формирование облика образца вооружения и военной техники на этапах научно-исследовательских и опытно-конструкторских работ / А.В. Радионов // Сборник научных трудов «Проблемы обороноспособности и безопасности», выпуск №19, ФГБНУ «Аналитический центр», 2018г. – С.76-79
6. Андрейчиков А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике: Учебник. – 2-е изд., дополненное и переработанное – М.: Финансы и статистика, 2004. 464 с.
7. Свид. 2019660121 Российская Федерация. Свидетельство об официальной регистрации программы для ЭВМ. Программа определения защищаемых элементов изделия /А.В. Радионов, В.А. Подсвиров, В.А. Мельник; заявитель и правообладатель А.В. Радионов (RU). – №2019619179; заявл. 17.07.2019; опубл. 30.07.2019, Реестр программ для ЭВМ. – 1 с.

Совершенствование организационной деятельности службы информационной безопасности на основе процессного подхода

В.Н. Соляной
Институт техники и цифровых технологий
Технологический университет
Г. Королев, МО, Россия
e-mail: solyanoy@ut-mo.ru

А.И. Сухотерин
Институт техники и цифровых технологий
Технологический университет
Г. Королев, МО, Россия
e-mail: sukhoterin@ut-mo.ru

Аннотация

Переход к процессному управлению требует от компаний функционального описания сфер деятельности их подразделений, но далеко не все на практике справляются с этой задачей. Однако, существуют определенные методы составления формализованного описания. Один из важных моментов – применение технического, организационного и правового анализа для организации деятельности Службы ИБ [1,2,3,4,5,6,7].

Анализируя в различных организациях положения о подразделениях ИБ, нередко отсутствуют в них ключевые разделы, например, раздела «Полномочия», а также с абстрактными формулировками функций и задач. Казалось бы, руководителю нет ничего проще, чем сформулировать в положении об отделе, какую работу он фактически выполняет (см. левый столбец табл. 1).

Как видно из табл. 1, в результате формализации все получается не так однозначно, как хотелось бы. Нетрудно увидеть различия между данными в левом и правом столбце, но вот как перейти от первого варианта ко второму? За кажущейся простотой темы скрывается весьма сложная методическая работа, которой часто не уделяется должного внимания.

Ключевые слова: информационная безопасность; прогнозирование; подразделение информационной безопасности; компетентность; процессный подход.

1.Введение

Для начала необходимо определить используемую систему ценностей – именно логически взаимосвязанную систему (например, такую, как на рисунке), а не фрагменты знаний из различных систем.

Примем, что в приведенной модели сфера деятельности рассматривается как работа, выполнение которой базируется на компетентности сотрудников и компетенциях подразделения (иногда вместо «сферы деятельности» употребляют термин «зона ответственности»). Навыки здесь в явной форме не указаны, поскольку они являются производными от умений [1,4,5,6,7].

Объекты – то, чем/кем управляет или что/кого контролирует подразделение. Объекты делятся на программное обеспечение, аппаратное, организационное и кадровое.

2. Функции и задачи подразделения

Функция – деятельность объекта в рамках некоторой системы и конкретные действия, совершаемые над управляемым или контролируемым объектом. В технике и в психологии, выражаясь обычным языком, функция обозначает принадлежность к чему-либо, что применяется для устремлений, решения задач, намерений, достижения цели. Функция может являться частью процесса. В рамках подразделения функции бывают основными и дополнительными.

Технологические основы построения интеллектуальных систем прогнозирования инцидентов информационной безопасности

В.Н. Соляной
Институт техники и цифровых технологий
Технологический университет
г. Королев, МО, Россия
e-mail: solyanoy@ut-mo.ru

А.И. Сухотерин
Институт техники и цифровых технологий
Технологический университет
г. Королев, МО, Россия
e-mail: sukhoterin@ut-mo.ru

Аннотация

Построение систем прогнозирования инцидентов информационной безопасности (ИБ) в настоящее время рассматривается как одна их сложных и важных задач стоящих перед руководством защищаемых информационных объектов в современных условиях ведения скрытой информационной войне как на межконтинентальных и континентальных пространствах, так и в региональных и локальных сферах применения различных информационных систем. Системы прогнозирования, которые позволяют осуществлять сбор информации и по ключевым признакам ее анализировать с целью выявления инцидентов информационной безопасности в соответствии с заданным методом их обнаружения и реализуемой стратегии информационной безопасности, а также осуществлять ответные действия. Наличие разномасштабных защищаемых информационных систем требует выработки разных подходов по выбору технологических основ построения наиболее целесообразных систем прогнозирования инцидентов информационной безопасности. Целью данной статьи является обоснование технологических основ построения, прежде всего интеллектуальных систем прогнозирования инцидентов информационной безопасности как наиболее эффективных в постоянно усиливающихся скрытых угроз для критически важных информационных инфраструктур. В статье предложен интеллектуальный подход построения систем прогнозирования инцидентов информационной безопасности в интересах реализации на защищаемых информационных объектах упреждающей стратегии обеспечения ИБ [Малюк]. Использование методов интеллектуальной аналитики позволяет снизить вычислительную сложность построения систем прогнозирования инцидентов, возникающих в неизвестный момент времени и оперативно выработать ответные действия.

Ключевые слова: информационная безопасность; прогнозирование; интеллектуальные подходы; инциденты; информационная система; критическая инфраструктура; методы; модель.

1. Введение

Интеллектуальные системы прогнозирования инцидентов информационной безопасности представляют собой совокупность базы знаний и базы данных о произошедших инцидентов информационной безопасности, математических и логических методов работы и программных средств, обеспечивающих сбор и обработку, анализ исходных данных в интересах прогнозирования инцидентов с целью выработки и принятия упреждающих управленческих решений по информационной безопасности. Поиск и своевременное выявление инцидентов информационной безопасности на основе предшествующих им возникновению различных аномальных активности рассматривается как одна из ключевых проблем в области информационной безопасности предприятий (организаций и учреждений). Такой поиск и выявление инцидентов в современных условиях реализуются различными подходами (методами). Используя новейшие информационные технологии обработки больших данных (Big Data) с различными методами обнаружения, распознавания и прогнозирования различных информационных ситуаций позволяют разрешать указанную выше проблему в области обеспечения информационной безопасности. Методы Big Data позволяют для анализа информационной обстановки задействовать и осуществлять сверку (на основе статистики) большого количества источников и прогнозировать возможные инциденты информационной безопасности с реализацией следующих технологий:

- обнаружения скрытых тенденций в больших наборах данных на основе их анализа;
- непосредственного прогнозирования различных ситуаций;
- вычислять вероятность любого возможного инцидента (исхода);
- оперативно получать желаемые результаты прогноза и др.

Наличия большого разнообразия в условиях и факторах защищаемых информационных системах для различных предприятий (организаций и учреждений) обуславливает привлечения разных алгоритмов построения целесообразных информационных систем прогнозирования инцидентов информационной безопасности. Литература по данной тематике представлена многочисленными разработками и обуславливает актуальность исследований в современном мире В последнее время в сфере исследований были рассмотрены большое количество различных подходов для построения адаптированных информационных систем прогнозирования инцидентов информационной безопасности на основе: прогнозирования изменений параметров временных рядов [4] сигнатурный метод и поиск по ключевым признакам[15], нейронные сети автоматического распознавания ситуаций [4]. и др. Адаптивная информационная система прогнозирования при функционировании в недетерминированной среде позволяет подстраиваться под изменение условий и ограничения окружающей анализируемой информационной среды.

Анализ существующих решений отражает индивидуальность использования разработанных подходов под конкретную информационную ситуацию и используемые методы, и системы прогнозирования. Следовательно, выявление и обоснование основ построения информационных систем прогнозирования инцидентов информационной безопасности с использованием различных условий и факторов функционирования защищаемых предприятий (организациях и учреждениях) является актуальной задачей.

2. Постановка задачи

Целью данной статьи следует рассматривать описание технологических основ построения интеллектуальных информационных систем прогнозирования инцидентов информационной безопасности для различных по масштабу деятельности предприятий (организаций и учреждений). Основной задачей работы является технологическое обоснование наиболее целесообразного подхода реализации с использованием метода интеллектуального анализа данных - нейросетевого прогнозирования.

Задачу исследования в данной постановке можно разделить на три уровня:

- стратегический уровень прогнозирования инцидентов. На данном уровне решается вопрос глобального прогнозирования (в интересах долгосрочного планирования информационной безопасности). Данная задача наиболее полно отражает потребности обеспечения информационной безопасности крупных распределенных предприятий (организаций и учреждений);
- тактический уровень прогнозирования инцидентов (в ходе краткосрочного планирования информационной безопасности). Данная задача прогнозирования тактического уровня сводится к решению задачи обеспечения информационной безопасности малых