ДИАГНОСТИКА ПСИХОФИЗИОЛОГИЧЕСКИХ ПОКАЗАТЕЛЕЙ ОПЕРАТОРОВ ИЕРАРХИЧЕСКИХ СИСТЕМ ВЫСОКОЙ ОТВЕТСТВЕННОСТИ В ЭКСТРЕМАЛЬНЫХ СИТУАЦИЯХ

Н.В. Пушкарева, В.А. Гущо

Диагностика должна позволять на ранних стадиях отслеживать отклонение психофизиологического состояния операторов расчетов сложных систем управления от нормы. Современное оборудование достоверно определяет даже малейшие сдвиги в анатомии и физиологии различных тканей организма. Однако обследование такими методами как ультразвуковое исследование, компьютерная томография, позитронно-эмиссионная томография и т.д. часто бывает дорогостоящим, громоздким и требует работы квалифицированных специалистов с медицинским образованием. При работе с лицами экстремальных видов деятельности требуется внедрение в практику работы новых методов и устройств для диагностики психофизиологического состояния (ПФС) человека в ходе выполнения поставленных задач. Необходимо применение других высокоточных, доступных для широкого использования и простых в эксплуатации технологий. При всем разнообразии аналитических методов, применяемых в современной медицине, все чаще ставится задача проведения превентивной диагностики [1]. Измерения в «боевых» условиях и в учебно-тренировочной работе требуют кратковременной, нетрудоемкой и информационной процедуры обследований. Всякая групповая деятельность, особенно операторская, протекает в условиях обратных связей. В этой взаимосвязанной деятельности любая акция одного члена группы вызывает «возмущение» в деятельности других, вынужденных сообразовываться с ней.

Системы группового слежения высокой ответственности включают в свой состав операторов, работающих не только на одном уровне иерархии. Повышение точности сопровождения в них основано на идее одновременной параллельной работы двух, а в общем случае и большего числа операторов. Такие системы представляют собой иерархические системы группового слежения (ИСГС) – это многоуровневые системы, включающие в свой состав нескольких операторов слежения. В ИСГС каждый оператор нижнего уровня включен в контур управления оператора верхнего уровня (более высокого). Под управлением понимается комплектование групп операторов и эргономическое обеспечение качества их работы. Для комплектования групп необходимо произвести подбор операторов, предрасположенных по своим психофизиологическим параметрам к групповой деятельности. В качестве диагностического устройства для подбора операторов предлагается дополнительно с гомеостатической системой использовать также иерархическую систему группового слежения. В качестве диагностического устройства на основе ИСГС могут применяться схемы Г. Татевосяна и А. Мелешева.

Литература

1. Бояркин М.А., Шапцев В.А. Об одном из подходов к решению проблемы «Человеческого фактора» на объектах нефтегазового комплекса [Электронный ресурс]. – Режим доступа: http://www.ipdn.ru/rics/doc0/DB/b3/3-boya.html. – Дата доступа: 19.05.2017.

ИНФОРМАТИЗАЦИЯ ОБЩЕСТВА И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ

Е.А. Свирский

Внедрение информационных технологий во все сферы деятельности общества стало нормой. И, очевидно, что обратного пути нет. Темпы развития и внедрения информационных технологий очень высоки. С одной стороны это радует, поскольку высокие темпы свидетельствуют об устойчивом движении общества к развитию и самосовершенствования, а со второй создает проблемы, связанные с освоением и пользованием инновационных технологий. Инновационные технологии далеко не всегда доведены до совершенства и могут стать источниками угроз безопасности для пользователей, как в плане несанкционированного предоставления доступа к ресурсам пользователей, так и личной безопасности пользователей.

Если реклама по новым продуктам информационных технологий активно распространяется самими производителями этих продуктов, то освещения вопросов безопасного их использования, особенно в сочетании с другими информационными

продуктами почти не ведется или эти вопросы обсуждаются только в профессиональной среде. До рядового пользователя существующие угрозы в популярных продуктах информационных технологий и возможные последствия их использования не доходят. Вообще говоря, даже лица в обязанности, которым вменено обеспечивать информационную безопасность, далеко не всегда осведомлены с существующими проблемами в сфере защиты информационных ресурсов и тем более защиты личности.

В настоящее время перед обществом встает серьезная проблема ликбеза в сфере защиты личности и информационных ресурсов, как общества в целом, так и отдельных пользователей. На государственном уровне этой проблеме достаточного внимания не уделяется. Необходимо выработать концептуальные основы повышения осведомленности общества в проблемах информационной безопасностью, и самым серьезным образом подойти к проблемам информационного зомбирования. Промедление в решении этих вопросов может серьезно повлиять на мотивационное поведение масс, защищенность государства от внешнего вмешательства в управление и устойчивое экономическое и политическое развитие государства.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОСНОВА ДЛЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

М.В. Сороко, А.М. Прудник

Рассматриваются практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом ISO/IEC 27001:2013 [1]. СМИБ – это часть общей системы управления организации, которая основана на оценке рисков, и которая предназначена для реализации, эксплуатации, мониторинга и совершенствования ИБ.

Перед разработкой СМИБ должно быть получено одобрение руководства для организации; должен быть разработан план проекта, который, в частности, предполагает определение области применения; определены требования, которым должна соответствовать СМИБ, должны быть определены информационные активы организации и получены данные по текущему состоянию ИБ в рамках области применения СМИБ; должна быть определена методология оценки рисков, сама оценка рисков и выбор вариантов действий с рисками (уменьшение, передача, принятие), а также выбор средств управления ими.

Собственно разработка СМИБ предполагает разработку конечной структуры организации с описанием ролей и сфер ответственности; разработку политик ИБ; разработку процедур обеспечения ИБ; разработку систем ИБ информационных и коммуникационных технологий и физических объектов, в том числе план внедрения средств управления; разработку средств управления; план проверок, проводимых руководством, т.е. список исходных данных для осуществления проверки и ее процедуры, включая аспекты аудита, мониторинга и измерения; разработку программы обучения, образования и информирования персонала организации в области ИБ, в т.ч. материалы для обучения в области ИБ, само обучение в области ИБ, включая разъяснение функций и ответственности, планы обучения и записи результатов обучения, образования и информирования в области ИБ и разработку конечного плана проекта СМИБ.

После разработки и внедрения СМИБ организации надлежит выполнить процедуры мониторинга и анализа, провести внутренний и внешний аудиты, произвести измерение результативности средств управления с целью определения их соответствия требованиям безопасности, а также выполнить оценки рисков.

Заключительными действиями являются разработка процедур по корректирующим и предупреждающим действиям, произвести проверку полного соответствия СМИБ по контрольной таблице стандарта ISO/IEC 27003 [2] и, при необходимости сертификации по национальному стандарту [3], провести внешний аудит.

Литература

1. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements // International Organization for Standardization. URL: https://www.iso.org/standard/54534.html (дата доступа: 17.05.2017).

2. ISO/IEC 27003:2017 Information technology – Security techniques – Information security