постепенных (деградационных) отказов. Этим вызван растущий интерес к постепенным отказам ППП. В работе [1] приведена методика индивидуального прогнозирования надежности ППП по постепенным отказам, позволяющая из партий однотипных приборов отобрать экземпляры, отвечающие требованию по надежности. Для повышения эффективности процедуры индивидуального прогнозирования актуальна ее автоматизация. При участии авторов разработано программное средство, включенное в систему автоматизированного расчета надежности электронных устройств АРИОН-плюс [2]. С программным средством автоматизации индивидуального прогнозирования надежности ППП по постепенным отказам и системой АРИОН-плюс можно ознакомиться на кафедре ПИКС БГУИР, обращаться по e-mail: bsm@bsuir.by или в ауд. 37 1-го учебного корпуса университета.

Список литературы

1. Боровиков С.М. Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники. М. : Новое знание, 2013. 343 с.

2. Разработка программного комплекса автоматизированной оценки надежности электронных устройств и систем: отчет о НИР (заключительный). Рук. С.М. Боровиков. Минск, 2016. 46 с. № госрегистрации 20121425.

ОБ ИЗУЧЕНИИ ВИДОВ И ОСОБЕННОСТЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ ВОЕННЫХ СПЕЦИАЛИСТОВ

Е.В. Валаханович, Л.В. Михайловская

В настоящее время военному специалисту необходимо соответствовать современным профессиональным требованиям в области защиты информации. Вследствие этого на кафедре высшей математики учреждения образования «Военная академия Республики Беларусь» разработаны и внедрены факультативный курс «Защита информации» и дисциплина «Прикладная математика». Одной из начальных тем вышеназванных курсов является тема «Классификация угроз информационной безопасности».

Авторы считают необходимым уточнение разработанной ранее, например, в [1], классификации угроз. Угрозы информационной безопасности в зависимости от характера ущерба, который они могут нанести, целесообразно систематизировать исходя из двух основополагающих критериев: происхождения и категорий безопасности. Предлагается угрозы по происхождению подразделить на два направления: стихийные (природного характера) и созданные людьми. Источники угроз информационной безопасности, созданные людьми, можно разделить на три типа: преднамеренные, техногенные и случайные. Угрозы по категориям безопасности соответственно делятся на три направления: угрозы нарушения целостности, конфиденциальности и доступности.

Так как средства и методы обработки, передачи и защиты информации постоянно совершенствуются, то перечень и классификация угроз информационной безопасности могут изменяться и приводить к появлению принципиально новых видов угроз и способов преодоления систем безопасности.

Таким образом, непрерывная и надежная работа по защите информации в сфере военной деятельности обусловлена разработкой классификации угроз информационной безопасности, как первого шага в алгоритме работы по их предотвращению и предупреждению.

Список литературы

1. Mehrhoff M. IT-Grundschutzhandbuch. Standard – Sicherheitsmapnahmen. Bundesamt fur Sicherheit in der Informationstechnik. DBUS-Jahrestagung, 2004.