УДК 681.3

ОЦЕНКА СПОСОБОВ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ ПРИ НАЛИЧИИ РИСКОВ ИСКАЖЕНИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ

ASSESSMENT OF WAYS OF PROTECTION OF COMPUTER SYSTEMS IN THE PRESENCE OF RISKS OF DISTORTION OF INFORMATION STREAMS

Шапошников В.Л.
кандидат физико-математических наук
Краснодарский кооперативный институт (филиал)
Российского университета кооперации
shaposh.vl@mail.ru

Умнова В.Е.
студент.
Краснодарский кооперативный институт (филиал)
Российского университета кооперации

Shaposhnikov V.L.
Candidate of physical and mathematical sciences.
Krasnodar cooperative institute (branch)
Russian university of cooperation
shaposh.vl@mail.ru

Umnova V.E.
Student.
Krasnodar cooperative institute (branch)
Russian university of cooperation

Аннотация: В работе рассмотрена оценка качества способов защиты бесперебойной работы компьютерных систем на основе применения показательного закона надежности.

Ключевые слова: компьютерные системы, закон надежности, способы защиты.

Annotation. In work the assessment of quality of ways of protection of trouble-free operation of computer systems on the basis of application of the indicative law of reliability is considered.

Keywords: computer systems, law of reliability, ways of protection.

Развитие вычислительной техники и создание на ее основе многочисленных компьютерных технологий широко применяемых в различных областях деятельности экономических субъектов, использующих информационные потоки в своей повседневной деятельности, явилось основанием для создания и применения различных способов защиты, используемых информационных систем [1].

Информация является дорогостоящим продуктом ,стоимость которого зачастую превосходит стоимость самих компьютерных информационных систем, включающих в себя аппаратные средства, информационно-коммуникационные технологии, проблемно-ориентированное программное обеспечение. Поэтому искажение или потеря информационных потоков, осуществляющих непрерывное функционирование в используемых компьютерных системах, наносит значительный ущерб в части функционирования самой компьютерной системы, принимаемым управленческим решениям с ее использованием и самому механизму функционирования экономического субъекта.

Факторами, влияющими на целостность информации, могут быть умышленные или вирусные искажения информационных потоков [2]. К сожалению, частота таких нарушений имеет тенденции к росту. Причем неправомерное уничтожение информации, дезорганизация процессов ее обработки, хранения и передачи наносит серьезный материальный и моральный ущерб как физическим лицам, так и компаниям. Помимо несанкционированного вмешательства в работу компьютерных систем широкое распространение имеет и создание компьютерных вирусов и вредоносных программ, которые работают по определенным сигналам. Вирусы имеют возможность размножаться и заражать другое программное обеспечение, а также базы данных.

Анализ угроз безопасности информации, которым подвергаются современные компьютерные системы, показал, что риск потери информационных потоков, который при создании систем защиты необходимо оценивать применительно к конкретной эксплуатируемой системе для правильного выбора способа ее защиты [3].

В настоящее время создано и имеется большое количество различных систем защиты информации, которые выполняют разнообразные функции, однако, при созда-

нии и эксплуатации компьютерных информационных систем надо объективно оценивать их защищенность [3].

Рассматривая корпоративные компьютерные системы, необходимо проводить анализ предполагаемых к использованию способов их защищенности, выявлять недостатки в защищенности различных элементов и всей компьютерной системы в целом. В связи с этим решение задачи по оптимальной архитектуре проектируемой системы необходимо принимать с учетом не только финансовых ресурсов направляемых на создание самой системы и ресурсов необходимых для организации ее защиты, но и требований в части ее бесперебойной работы. Выбор способа защиты системы от предполагаемых угроз потери целостности информационных потоков надо делать исходя из критериев, определяемых проектом системы и условий ее эксплуатации. Качество способа защиты оценивается по показателям, определяемым на основе методики расчетов адекватно учитывающей риски угроз, которые влияют на бесперебойную работу системы в целом и функционирование ее составляющих элементов [4].

Для оценки способов защиты корпоративных компьютерных систем, функционирование которых регламентировано технологией их эксплуатации предусматривающей учет времени безотказной работы, на основании выполненного анализа работ по защите их эксплуатации, целесообразно использовать методику основанную на применении показательного закона надежности, позволяющего учитывать интенсивность отказов как элементов системы, так и системы в целом. Приемлемым способом защиты можно считать тот, который, например, удовлетворяет заданным условиям бесперебойной работы согласно требований проекта компьютерной системы. Применение данной методики оценки различных способов защиты позволяет своевременно проводить обновление применяемого способа или его замену. Анализ использования различных способов защиты компьютерных систем показал, что эффективность защиты информационных потоков в компьютерных системах, как правило, достигается не количеством затраченных финансовых ресурсов на их приобретение и организацию, а способностью применяемого метода адекватно реагировать на возникающие угрозы информационным потокам функционирующим в созданной компьютерной системе и попытки несанкционированного доступа к ним. Опыт показывает, что мероприятия по защите информации в эксплуатируемых компьютерных системах должны носить комплексный характер, т.е. выбор способа защиты информации ,основным критерием которого является бесперебойная работа системы, должен сопровождаться различными мерами противодействия угрозам включающие правовые, организационные и программно-технические. Каждый пользователь компьютерной информационной системы должен иметь тот объем полномочий по доступу к информационным потокам, который предусмотрен выбранным способом защиты, оценка которого соответствует максимальному времени бесперебойной работы системы.

Литература:

1. Мельников В.И. Защита информации в компьютерных системах / В.И. Мельников. – М. : Финансы и статистика, 1997.

2. Фролов А.В. Осторожно компьютерные вирусы / А.В. Фролов, Г.В. Фролов. – М. : Диалог-МИФИ, 1996.

3. Безбогов А.А. Методы и средства защиты компьютерной информации / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов : ТТГУ, 2006.

4. Вентцель Е.С. Теория вероятностей / Е.С. Вентцель. – М. : Наука, 1969.

References:

1. Melnikov V.I. Information security in computer systems / V.I. Melnikov. – M. : Finance and statistics, 1997.

2. Frolov A.V. Ostorozhno computer viruses / A.V. Frolov, G.V. Frolov. – M. : Dialogue MEPhI, 1996.

3. Bezbogov A.A. Methods and means of protection of computer information / A.A. Bezbogov, A.V. Yakovlev, V.N. Shamkin. – Tambov : TTGU, 2006.

4. Venttsel E.S. Teoriya veroyatnostey / E.S. Venttsel. – M. : Science, 1969.