Д.А.Васюкова (4 курс, каф. НБ), Д.Е.Сипович, ст. преп.

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УПРАВЛЕНИИ ПРЕДПРИЯТИЕМ

Информационная безопасность достигается комплексом мероприятий, позволяющим обеспечивать следующие свойства информационных процессов:

- конфиденциальность – возможность ознакомится с информацией (именно с данными или сведениями, несущими смысловую нагрузку, а не последовательностью бит их представляющих) имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями;
- целостность – возможность внести изменение в информацию (речь идет о смысловом выражении) должны иметь только те лица, кто на это уполномочен;
- доступность – возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.
- учет – т.е. все значимые действия лица, выполняемые им в рамках, контролируемых системой безопасности (даже если они не выходят за рамки определенных для этого лица правил), должны быть зафиксирован и проанализированы;
- непререкаемость или аппелируемость – характерно для организаций, в которых функционирует обмен электронными документами с юридической, финансовой или другой значимостью), т.е. лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения [1].

Обеспечение требуемого уровня безопасности может быть достигнуто двумя подходами:

1. Подход, обеспечивающий реализацию выше перечисленных свойств, основан на комплексе запретов. Такой подход приводит к тому, что чем меньше работает вычислительная система, тем она безопаснее. Самая безопасная система именно та, которая не работает.
2. Подход, обеспечивающий реализацию выше перечисленных свойств, основан на инвариантности вычислительных процессов к разрушающим воздействиям как извне, так и изнутри ВС и способности гарантированно решать поставленную задачу в условиях разрушения среды функционирования. Такое функционирование возможно в условиях адекватности модели функционирования вычислительной системы программно-аппаратной среде. Мерой адекватности является полнота учёта закономерностей рассматриваемой предметной области.

В качестве этой закономерности целесообразно рассматривать закон сохранения целостности, сформулированный в работах [1-3].

Закон сохранения целостности объекта (ЗСЦО) – устойчивая повторяющаяся связь свойств объекта и свойств действия при фиксированном предназначении. Проявляется ЗСЦО во взаимной трансформации свойств объекта и свойств его действия при фиксированном предназначением. Модель объекта – процессор. Модель действия – программа в действии. Заданное предназначение – требуемое количество требуемых символов, преобразованных в памяти ВС.

Не учитывая на практике закон сохранения целостности вычислительной системы, мы сталкиваемся с тем, что результат применения созданной нами вычислительной системы не соответствует ожидаемому.

Новизна предлагаемого подхода заключается в принципиально ином рассмотрении внешних и внутренних факторов, имеющих место при работе программно-аппаратной системы. То есть, в функционирование программно-аппаратной системы вводится понятие объективной реальности, которое ранее находило ничтожно малое отражение при реализации алгоритмической части программы и, в конечном итоге, подменялось

понятием «целевое назначение». Если же объективной реальности уделить должное внимание и так же, как и требования к программному обеспечению и атрибутам информации, провести через методологический, методический и технологический уровни, то получится, по сути, та же модель информационной системы, но с дополнительным третьим и очень важным компонентом. Структурная схема представлена на рис. 1.

Учитывая объективную реальность при работе программно-аппаратной среды уже на методологическом уровне появляется понятие мироустройства. Современная наука уже давно рассматривает и изучает объекты и их движение (статика и динамика), но еще нигде не предложен физико-математический аппарат о том, когда законы статики и динамики начинают действовать. Именно на этой грани и находиться мироустройство, которое при переходе на методический уровень, превращается в более осязаемое свойство целостности. Однако, эта не та целостность, что описывается в современных курсах защиты информации, и введенная в качестве необходимости. Эта другая целостность, которая находит совершенно иное математическое отражение. Именно эта целостность позволяет связать в единую модель структурность и изменчивость, как промежуточные абстракции. Это позволяет при переходе на технологический уровень вывести условие замыкания между моделью объекта и моделью действия.

Рис. 1

Предлагаемая модель, идея которой описана с использованием объективной реальности, позволяет понизить роль администратора до функций контроля работоспособности, подняв проблему коррекции программно-аппаратных ошибок, пусть даже вызванных целенаправленно, на автоматический уровень.

ЛИТЕРАТУРА:

1. Бурлов В.Г. Об оценивании эффективности обеспечения информационной безопасности в контуре управления социально-экономическим образованием. В кн. «Фундаментальные исследования и

иннвации в технических университетах». Секция 15. Национальная безопасность, стр. 29-30, – С-Пб. С-ПбГТУ, 2007.
2. Бурлов В.Г. Синтез модели вычислений в условиях разрушения программно-аппаратной среды. Сборник алгоритмов ипрограмм типовых задач. Выпуск 20, под ред. Кудряшова И.А., стр. 187- 203, – СПб, МО РФ, 2002.
3. Бурлов В.Г. Основа гарантированного управления риском – структурно – функциональный синтез модели потенциально опасного объекта. В кн. «Фундаментальные исследования в технических университетах». Том 2. Национальная безопасность, стр. 137-150, – С-Пб. С-ПбГТУ, 2002.