О. В. Л у к и н о в а (Москва, ИПУ РАН)**. Методы компьютерного управления защитой распределенной корпоративной сети.**

На сегодняшний день значительная часть бизнес-процессов компании реализуется на базе ИТ-технологий. Поэтому и корпоративные сети следует рассматривать как совокупность бизнес-процессов, реализованных в сетевой среде. Тогда в соответствии с [1] под защищаемым активом понимается перечень взаимосвязанных потоками информации автоматизированных функций, потребителей бизнес-процесса и ресурсов, необходимых для функционирования функций и потоков. При этом элементам бизнес-процесса ставятся в соответствие: функциям и потребителям — приоритеты P, ресурсам и потокам — уязвимости $\widetilde{X}$ (модель уязвимостей описана в [2]). Пример такого бизнес-процесса приведен на рис. 1.

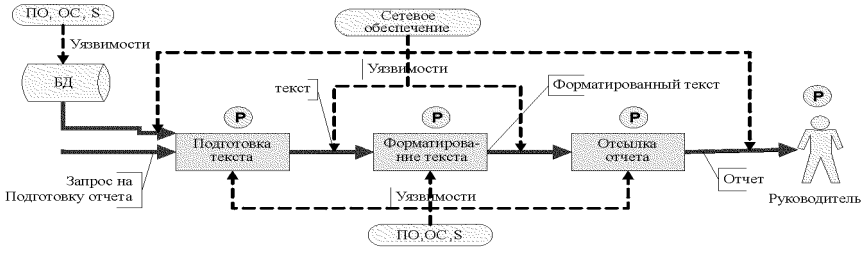

Рис. 1. Схема бизнес/процесса с указанием Приоритетов и Уязвимостей: ПО — программное обеспечение, ОС — системное обеспечение, S — аппаратное обеспечение. Сплошные стрелки обозначают информационные потоки, пунктирные — связи ресурсов с функциями и потоками

Указанные параметры позволяют построить систему безопасности $S = \langle\{\overline{KS}\}, \{\overline{KS}(Tr^l)\}, \{pz_i\}\rangle$, где $\{pz_i\}$ — средства защиты (СЗ), реализующие сервисы безопасности для активов, $\{\overline{KS}(Tr^l)\}$ — требования безопасности, в соответствии с которыми произведен выбор средств $\{pz_i\}$, $\{\overline{KS}\} = \{C, D, K\}$ — принятые в системе критерии безопасности по целостности, доступности и конфиденциальности соответственно, определяющие выбор требований $\{\overline{KS}(Tr^l)\}$. Каждому бизнес-процессу (и его элементам) на основании P и $\widetilde{X}$ ставятся в соответствие определенные уровни критериев K, C, D, которые обеспечиваются функционированием системы безопасности и, вообще говоря, нарушены быть не могут.

Если при нападении на актив система S не сработает и атака реализуется, то это будет означать, что критерии безопасности нарушены и бизнес-процесс не может выполняться корректно или простаивает вовсе. Тогда необходимо решить следующие задачи, подробное описание которых приведено в [1], [3], а схема управления — на рис. 2.

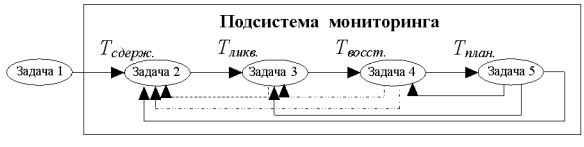

Рис. 2. Циклическая схема управления защитой РКС

З а д а ч а 1. Оптимальное планирование СЗ бизнес-процесса от вторжения или вирусного заражения.

З а д а ч а 2. Оптимальное управление оперативными СЗ при обнаружениях атаки для ее сдерживания с учетом фазы атаки.

З а д а ч а 3. Ликвидация факта вторжения.

З а д а ч а 4. Восстановление целостности ресурсов бизнес-процессов после ликвидации атаки.

З а д а ч а 5. Оптимальное перепланирование средств $\{pz_i\}$ после ликвидации атаки с учетом модифицированной модели $\widetilde{X}$.

В работе сформулированы критерии оценки, ограничения и методы, позволяющие производить компьютерную оценку возможности автоматического восстановления работоспособности бизнес-процессов, реализованных в сетевой среде.

СПИСОК ЛИТЕРАТУРЫ

1. *Лукинова О. В.* Формализация задачи планирования защиты распределенной компьютерной сети на основе бизнес-процессного подхода. — Надежность (в печати).
2. *Лукинова О. В.* Формирование модели угроз безопасности компьютерной сети при бизнес-процессном подходе. — В сб.: Труды XII научно-практической конференции «Реинжиниринг бизнес-процессов на основе современных информационных технологий». Москва, 2009, с. 170–176.
3. *Лукинова О. В.* Задачи управления защитой активов распределенной компьютерной сети при обнаружении атаки. — Надежность (в печати).