сти, а также выдвинуть математически и логически обоснованные предложения по использованию конкретного сценария развития Республики Беларусь в долгосрочной перспективе.

На основе полученных прогнозных результатов проводится качественное и количественное описание положения рассматриваемых регионов в течение прогнозируемого периода и разрабатываются рекомендации по проведению эффективной государственной инновационной политики в экономической, социальной и экологических сферах.

Наибольшая трудность, возникающая при работе с предлагаемой моделью связана с огромным объёмом информации (статистической и определяемой экспертным путём), необходимым для просчёта всех необходимых показателей, взаимосвязей и взаимозависимостей.

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ КОРПОРАТИВНЫХ СИСТЕМ

Судник Д. П., Першин М. А.
Бобруйский филиал БГЭУ
Руководитель: Смоглюков Н. И.

Компьютерные корпоративные системы, открывая новые возможности обработки информации, в то же время становятся одной из уязвимых сторон защиты конфиденциальности информации и ее целостности.

В отсутствие защиты частные и корпоративные сети могут подвергаться несанкционированному мониторингу. При минимальной или вовсе отсутствующей защите интрасети возможны внутренние вторжения, а соединения с Интернетом и внешними сетями могут представлять опасность для частных сетей.

Некоторые атаки являются пассивными, т. е. используются для мониторинга информации, а другие – активными, т. е. имеют целью повреждение или уничтожение информации или самой сети.

Как правило, большинство сетевых сеансов проводится в незащищенном режиме, что позволяет злоумышленнику, имеющему доступ к путям передачи данных, «прослушивать», или интерпретировать (читать), трафик.

После того, как злоумышленник прочтет данные, его следующим шагом может стать их модификация. Данные в пакете можно изменить так, что об этом не узнает ни отправитель, ни получатель.

В большинстве сетей и операционных систем компьютер идентифицируется по его IP-адресу. В определенных ситуациях IP-адрес можно сфальсифицировать, что приведет к неправильной идентификации. Кроме того, специальные программы способны создавать IP- пакеты, которые кажутся отправленными с допустимых адресов внутри корпоративной интрасети.

Общий знаменатель большинства операционных систем и планов сетевой защиты - управление доступом на основе паролей.

При атаке типа «Отказ в обслуживании» в отличие от предыдущего варианта вторжения нарушается нормальная работа компьютеров или сети для обычных пользователей – они получают отказ в обслуживании.

При атаке посредника между системой и клиентом, ведущих коммуникационную связь, находится некто, осуществляющий мониторинг и захват данных, а также полностью контролирующий соединение.

Атака по скомпрометированному ключу. Получение ключа – процесс для злоумышленника трудный и ресурсоемкий, но возможный. Ключ, добытый злоумышленником, называется скомпрометированным.

Атака с использованием сетевого анализатора. Сетевой анализатор, или, как его еще называют, «ищейка»(sniffer), - это приложение или устройство, способное читать, отслеживать и перехватывать сетевые пакеты.

Атака на уровне приложения направлена на серверы приложений с целью вывести их из строя за счет нарушения работы серверной операционной системы или самих приложений.

Наиболее простыми и дешёвыми являются административные методы защиты, как то использование в сети стойкой криптографии, статических ARP-таблиц, hosts-файлов вместо выделенных DNS-серверов, использование или неиспользование определённых операционных систем и другие методы.

Следующая группа методов защиты от удалённых атак – программно-аппаратные. К ним относятся:

- программно-аппаратные шифраторы сетевого трафика;
- методика Firewall;
- программные средства обнаружения атак (IDS – Intrusion Detection Systems или ICE – Intrusion Countermeasures Electronics);
- программные средства анализа защищённости (SATAN – Security Analysis Network Tool for Administrator, SAINT, SAFEsuite, RealSecure и др.);

защищённые сетевые ОС.

В общем случае методика Firewall реализует следующие основные функции:

1. Многоуровневая фильтрация сетевого трафика;
2. Proxy-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте. Смысл proxy-схемы заключается в создании соединения с конечным адресатом через промежуточный proxy-сервер на хосте Firewall;
3. Создание приватных сетей с "виртуальными" IP-адресами. Используется для скрытия истинной топологии внутренней IP-сети.

Здесь можно выделить подгруппу методов защиты – программные методы. К ним относятся прежде всего защищённые криптопротоколы, используя которые можно повысить надёжность защиты соединения.