их замещения необходимо увеличивать посевы соответствующих яровых культур [5].

Задача (1)—(6) является задачей линейного булевого программирования и решается стандартными методами с помощью известных математических программных пакетов, например Matlab. Результатом ее решения является вектор X, определяющий размещение сельскохозяйственных культур по участкам хозяйства и используемые технологии возделывания.

Таким образом, применение математических методов позволяет осуществить оперативное репланирование производства сельскохозяйственных культур и, соответственно, снизить ущерб, нанесенный неблагоприятными погодными условиями. При предварительной страховке посевов можно еще больше снизить или вообще устранить экономический ущерб, нанесенный посевам, при условии, если страховое возмещение достаточно для восстановления посевов.

ЛИТЕРАТУРА

1. *Официальные* данные министерства сельского хозяйства РФ за период 01.01.2006—15.03.2006.
2. *Кульба В. В., Утепбергенов И. Т., Швецов А. Р.* Модели и методы планирования и репланирования сельскохозяйственного производства в условиях чрезвычайных ситуаций // Тез. докл. участников II междунар. конф. «Безопасность и экология горных территорий». — Владикавказ, 1995. — С. 214—218.
3. *Утепбергенов И. Т.* Модели и методы создания автоматизированных систем информационного обслуживания и управления отраслями сельскохозяйственного производства Республики Казахстан: автореф. дис. д-ра техн. наук. — М., 1995.
4. *Обиралов А. И.* Дешифрирование снимков для целей сельского хозяйства. — М.: Недра, 1982
5. *Дюрягин И. В.* Земледелие. — Курган: КГСХА, 1997.

☎ *(495) 334-90-09*

E-mail: sti82@mail.ru ❑

УДК 658.012.011.56

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ РЕГИСТРАЦИИ ИНФОРМАЦИИ ДЛЯ ОТРАЖЕНИЯ УДАЛЕННЫХ АТАК

М. А. Шелков(1), М. Ю. Гладков(2)

[1] *Институт технологии, экономики и предпринимательства Московского энергетического института (технического университета)*

[2] *Институт проблем управления им. В. А. Трапезникова, г. Москва*

Развитие автоматизированных систем на основе глобальных телекоммуникаций привело к росту их уязвимости от внешних вторжений или сетевых атак. Под сетевой атакой понимается действие, предпринимаемое злоумышленником для получения несанкционированного удаленного доступа к ресурсам автоматизированной системы или корпоративной (локальной) сети с целью вызова отклонения от нормального протекания информационного процесса или хищения данных[1]. Удаленная сетевая атака заключается в попытке проникновения в систему через сеть (например, Интернет) с удаленного компьютера.

По субъекту удаленной атаки различают атаки, выполняемые при постоянном участии человека, и атаки, выполняемые специально разработанными программами без непосредственного участия человека. В первом случае для воздействия на автоматизированную систему может использоваться и стандартное программное обеспечение, во втором — практически всегда применяются специально разработанные программы.

По характеру источников уязвимости автоматизированных систем атаки можно подразделить на атаки, основанные на:

— недостатках системы обеспечения информационной безопасности или просчетах при разработке политики безопасности;

— ошибках оперативного управления различными видами обеспечения автоматизированных систем (в первую очередь системного администрирования);

— недостатках алгоритмов защиты, реализованных в системе обеспечения информационной безопасности.

По физической дислокации объекта вторжения можно выделить атаки на информацию:

[1] *Информационная* безопасность систем организационного управления. Теоретические основы: в 2 т. / Под ред. Н.А. Кузнецова, В.В. Кульбы. — М.: Наука, 2006. — Т. 1. — 495 с.

— хранящуюся на внешних запоминающих устройствах;

— передаваемую по линиям связи;

— обрабатываемую в основной памяти компьютера.

По характеру воздействия на объект можно выделить атаки с пассивным и активным воздействием. Под пассивным понимается воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Отсутствие непосредственного влияния на работу системы существенно затрудняет обнаружение атак данного типа. Активным называется воздействие на автоматизированную систему, которое оказывает непосредственное влияние на ее работу. Как показывает практика, большинство удаленных атак являются активными воздействиями.

К самым распространенным в настоящее время средствам защиты относятся межсетевые экраны, средства антивирусной защиты, системы аутотентификации и средства предотвращения удаленных вторжений. Одна из главных составляющих функционирования таких средств — процедура регистрации и последующей обработки данных по наиболее критичным событиям в системе обеспечения безопасности, причем для предотвращения сетевых вторжений данная процедура носит ключевой характер.

Регистрационные данные дают возможность анализировать взаимодействие автоматизированной системы с внешними сетями и пользователями, выявлять источники уязвимости автоматизированных систем, обнаруживать несанкционированные или недопустимые действия как со стороны внешней информационной среды, так и внутренних пользователей. Все это обеспечивает возможность постоянного мониторинга состояния автоматизированной системы с точки зрения информационной безопасности в режиме реального времени. Регистрационные данные, создаваемые операционными системами, приложениями, межсетевыми экранами, средствами антивирусной защиты и средствами предотвращения вторжений, содержат информацию, необходимую для решения комплекса проблем обеспечения информационной безопасности.

В функции системы регистрации входят идентификация и фиксация в специализированном регистрационном журнале событий и процессов, происходящих в автоматизированной системе. Накапливаемая в регистрационном журнале информация предназначена для использования в целях анализа и контроля за действиями внешних и внутренних пользователей автоматизированной системы, выявления несанкционированных внешних воздействий на систему, а также выявления попыток или случаев нарушения регламента работы пользователей в системе, включая «взлом» механизмов защиты и т. д.

Система регистрации — комплекс технических, информационных, программных и организационных средств, обеспечивающий идентификацию состояний системы обработки данных в произвольные моменты времени. Одна из основных целей системы состоит в выявлении (идентификации) факта удаленной сетевой атаки на автоматизированную систему. Анализ принципов построения систем регистрации позволяет выделить следующие основные типы этих систем.

Под *детерминированной системой регистрации* понимается такая система, когда в определенных, заранее выбранных точках контроля фиксируются по определенному алгоритму действия, происходящие в данной точке. Под точкой контроля понимается точка в автоматизированной системе, определяемая на уровне процедуры, операции, совокупности или элемента данных, сервера, автоматизированного рабочего места, запоминающего устройства и др., в которой ведется собственно регистрация. Фиксирование производится постоянно либо в определенные, заранее выбранные отрезки времени.

Одним из эффективных методов регистрации является *случайная регистрация*, под которой понимается контроль некоторого процесса в выбранной случайным образом точке либо контроль событий и действий внешних и внутренних пользователей, а также событий и процессов, происходящих в системе через случайные промежутки времени.

Формализованная методология проектирования детерминированных систем регистрации базируется на применении математического аппарата теории графов, основой методов разработки систем случайной регистрации служит теория игр.

В настоящее время системы регистрации развиваются в направлении создания специализированных средств анализа зарегистрированных событий и подготовки оперативных решений по блокированию попыток взлома системы защиты данных или иных нарушений регламента работы, методов планирования и управления процессами ликвидации последствий нештатных ситуаций, вызванных удаленными атаками. Упомянутые средства чаще всего объединяются в отдельную подсистему, компоненты которой распределены по всей автоматизированной системе.

Основные структурные элементы такой подсистемы:

— средства управления процессом регистрации;

— средства сбора регистрационных данных и источники событий безопасности;

— сервер обработки данных о зарегистрированных событиях;

— специализированная база данных о зарегистрированных событиях;

— рабочее место администратора.

Основные функции подсистемы заключаются в сборе и хранении регистрационных данных, обработке данных по зарегистрированным событиям, автоматизированном анализе регистрационных данных, оперативном отображении событий в автоматизированной системе, автоматизированной разработке и ведении базы сценариев развития нештатных ситуаций, ведении базы данных типовых решений, автоматическом формировании рабочих планов по ликвидации последствий нештатных ситуаций, связанных с нарушениями режима информационной безопасности на основе результатов автоматизированного анализа регистрационных данных.

☎ *(495) 334-89-09*

E-mail: shelkov_m@mail.ru ❑