СЕКЦИЯ В.ТЕОРИЯ И МЕТОДИКА ТЕХНОЛОГИЧЕСКОГО И ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ

Т.ХАКИМОВА.,А. ЕМЕЛ

Казахский национальный университет им.аль-Фараби,г.Алматы,Казахстан

О РОЛИ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ

В обучении курса информационных технологий для профессиональных целей в Казахском национальном университете им.аль-Фараби, рассматривается тема «Основные методы защиты информации в локальных сетях».Доклад посвящен на тему: Защита в локальных сетях. Программные средства индивидуальной защиты информации. Использование экспертных систем для распознавания попыток несанкционированного доступа.

Цель доклада раскрыть тему: основные методы защиты информации в локальных сетях.Изучения темы обусловлена факторами высокие темпы роста парка персональных компьютеров, применяемых в самых разных сферах деятельности; расширение круга пользователей, увеличение объемов информации различного назначения и различной принадлежности; бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности; повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные; развитие глобальной сети Internet. Задача:Использования современных информационных технологии в подготовке высококвалифицированных специалистов по различным направлениям. Роль и место системы обеспечения защиты информации в локальных сетях в системе национальной безопасности РК.

Практическое применения: Для повышения эффективности, качество в подготовке высококвалифицированных специалистов.

Ключевые слова:Персональный компьютер,информационная технология,информация, защита информации,безопасность информации.

Актуальность темы обучения студентов инновациям в условиях Республики Казахстан.

Обеспечение надежной защиты корпоративной сети-сложный процесс, который представляет собой непрерывную и постоянную последовательность действий по реализации комплекса мер информационной безопасности.

Одним из основных компонентов системы защиты корпоративной сети являются межсетевые экраны, которые обеспечивают организацию защитного периметра, защищающего информационные ресурсы организации от доступа извне и контролирующего процедуры взаимодействия пользователей корпоративной сети с внешними сетями, в основном с Интернетом. Межсетевой экран обеспечивает решение таких задач, как защита локальной сети от несанкционированного доступа из внешних сетей, безопасный доступ в Интернет корпоративных пользователей, удаленное подключение пользователей к ресурсам корпоративной информационной системы. Антивирусные продукты обеспечивают надежную защиту серверов, рабочих станций, почтовых систем и Интернет-трафика от поражения компьютерными вирусами.Система организации защищенного удаленного доступа пользователей к ресурсам корпоративной сети предоставляет возможность создания защищенных Интернет-каналов, реализованных на базе технологии построения виртуальных частных сетей, что обеспечивает высокий уровень безопасности корпоративного трафика при небольших финансовых затратах.Системы обнаружения вторжений и системы анализа защищенности ресурсов корпоративной сети, работающие в едином комплексе, обеспечивают предотвращение хакерских атак, позволяют предупреждать внешние и внутренние хакерские атаки, контролируют

проходящий трафик и процессы на ключевых серверах сети, дают возможность в автоматическом режиме блокировать атаки, обнаруживать и устранять уязвимости в системе защиты корпоративной сети. Средства управления политикой безопасности и защиты от несанкционированного доступа реализуют комплексные решения для организации доступа пользователей и администраторов к ресурсам корпоративной сети, предусматривают использование электронных ключей с уникальными персональными идентификаторами пользователей, электронных замков и других средств защиты серверов,рабочих станций и телекоммуникационного оборудования от несанкционированного доступа.

Основной задачей системы управления политикой безопасности и защиты от несанкционированного доступа является обнаружение фактов несанкционированных действий пользователей корпоративной сети на основе сбора и анализа информации о событиях, регистрируемых на информационных ресурсах корпоративной сети.В задачу этой системы входит сбор информации о следующих событиях:

- изменение файловой системы контролируемого узла корпоративной сети;
- использование внешних устройств ввода-вывода (дисководов, USB-устройств и т.п.);
- запуск и остановка процессов на контролируемом узле;
- локальная либо удаленная регистрация начала сеанса работы пользователя, а также завершение работы пользователей;
- использование принтеров и других периферийных устройств;
- ведение статистики использования сетевых сервисов;
- изменение аппаратной и программной конфигурации контролируемого узла.

Система управления политикой безопасности и защиты от несанкционированного доступа имеет распределенную архитектуру и

включает такие компоненты, как программные сенсоры, сервер управления сенсорами и консоль администратора. Консоль администратора служит для централизованного управления сервером управления сенсорами и сенсорами системы, отображения результатов работы системы и формирования отчетов. Использование средств защиты, как межсетевые экраны, системы контроля доступа пользователей и т.п., не дает полной гарантии устойчивости корпоративной сети к атакам. Любое программное или аппаратное обеспечение не является совершенным, и в нем имеются уязвимости, позволяющие совершить какие-либо действия в нарушение установленного порядка использования информационных ресурсов. Своевременное обнаружение попыток взлома информационных ресурсов и оперативная реакция на эти действия позволяют значительно повысить уровень защищенности сети [2;71].

Система обнаружения и предотвращения вторжений

Данная система позволяет обнаруживать атаки и злоупотребления в отношении узлов корпоративной сети компании. Система может обеспечивать как защиту конкретного узла, так и целого сетевого сегмента. Основной принцип работы системы обнаружения и предотвращения вторжений заключается в выявлении и блокировании сетевых атак в корпоративной сети на основе анализа пакетов данных, циркулирующих в этой сети, и в последующем выявлении аномалий сетевого трафика сети. Система позволяет с равной степенью эффективности выявлять и блокировать атаки со стороны как внешних, так и внутренних нарушителей.Для обнаружения вторжений система использует метод, основанный на выявлении сигнатур известных атак, а также метод, базирующийся на анализе поведения сети. Метод, основанный на выявлении сигнатур, обеспечивает обнаружение атак посредством специальных шаблонов. В качестве сигнатуры атаки могут выступать строка символов, семантическое выражение на специальном языке,

формальная математическая модель.При получении исходных данных о сетевом трафике корпоративной сети система проводит их анализ на соответствие определенным шаблонам или сигнатурам атак, хранимым в постоянно обновляющейся базе данных системы,при обнаружения сигнатуры в исходных данных система фиксирует факт обнаружения сетевой атаки и блокирует ее дальнейшие действия.

Для выявления новых типов атак в системе обнаружения вторжений реализован метод, который основан на анализе поведения корпоративной сети и использует информацию о штатном процессе функционирования корпоративной сети. Принцип работы этого метода заключается в обнаружении несоответствия между текущим режимом функционирования корпоративной сети и моделью штатного режима работы, заложенной в параметрах работы метода.В состав системы обнаружения и предотвращения вторжений входят следующие компоненты: сетевые сенсоры, серверные сенсоры, датчики, сервер управления сенсорами, а также консоль администратора. Сетевые сенсоры, предназначенные для защиты объектов сетевых сегментов корпоративной сети, обеспечивают перехват и анализ всего сетевого трафика, передаваемого в рамках того сегмента, где они установлены. Серверные сенсоры устанавливаются на серверы корпоративной сети и обеспечивают защиту определенных сетевых сервисов сети. В числе таких сенсоров могут быть серверные сенсоры для почтовых, файловых и Web-серверов, а также для серверов баз данных. На одном сервере корпоративной сети может быть одновременно установлено несколько типов сенсоров. Датчики выполняют функции управления серверными и сетевыми сенсорами, а также функции обеспечения передачи информации между сенсорами и сервером управления сенсорами. Сервер управления сенсорами обеспечивает централизованный сбор, хранение и анализ информации, поступающей от серверных и сетевых сенсоров, и дает возможность выявления

распределенных сетевых атак на основе анализа полученной информации. Консоль администратора предназначена для централизованного управления компонентами системы и отображения результатов работы системы. Сообщение об обнаруженной атаке,формируется в соответствии со стандартом IDMEF (Intrusion Detection Message Exchange Format) и содержит следующую информацию:

- дата и время обнаружения атаки;
- общее описание атаки, включая возможные ссылки на дополнительные источники информации о выявленной атаке;
- символьный идентификатор атаки по классификатору CVE (Common Vulnerabilities Exposures, http://cve.mitre.org) или CERT (Computer Emergency Response Team, http://www.cert.org/);
- уровень приоритета обнаруженной атаки (низкий, средний или высокий);
- информация об источнике атаки (IP-адрес, номер порта, доменное имя и др.);
- информация об объекте атаки (IP-адрес, номер порта, доменное имя и др.);
- рекомендации по устранению уязвимости, в результате которой был зафиксирован факт реализации атаки.

Система анализа защищенности корпоративной сети

Система анализа защищенности предназначена для проведения регулярных, всесторонних или выборочных тестов с целью выявления и устранения уязвимостей программно-аппаратного обеспечения корпоративной сети: сетевых сервисов, операционных систем, прикладного программного обеспечения, систем управления базами данных, маршрутизаторов, межсетевых экранов, а также для проверки наличия последних модулей обновления и т.п. В состав системы анализа защищенности входят сканеры безопасности, предназначенные для

проведения заданного множества проверок в соответствии с параметрами, определенными администратором безопасности; сервер хранения результатов работы системы; консоль администратора для централизованного управления системой.

Сканер безопасности представляет программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них уязвимостей, использование которых может привести к компьютерным нарушениям.Сканеры безопасности сокращают время, необходимое для поиска уязвимостей, за счет автоматизации операций по оценке защищенности систем. Принципы работы сканера, основной модуль программы подсоединяется по сети к удаленному компьютеру. В зависимости от активных сервисов формируются проверки и тесты. Найденная при сканировании каждого порта служебная информация сравнивается с таблицей правил определения сетевых устройств, операционных систем и возможных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии потенциальной уязвимости.Любое изменение конфигурации корпоративной сети компании, а также сетевого программного обеспечения должно быть исследовано системой анализа защищенности. Работа системы основана на анализе сетевого трафика с использованием метода сигнатур, поэтому система анализа защищенности требует постоянного обновления базы уязвимостей. В настоящее время многие компании, занимающиеся вопросами информационной безопасности (например, Internet Security Systems и др.), предлагают стратегию применения описанных систем в составе единых комплексов, позволяющих осуществлять централизованное управление информационной безопасностью корпоративной сети. Для повышения качество изучаемого материала предлогается,вопросы для закрепления:

1. Что могут сделать компании для защиты корпоративной сети?

2. Чем обусловлена сложность создания системы защиты информации?
3. Что входит в компоненты сетевой системы защиты?
4. Что выполняют межсетевые экраны?
5. Пояснить цели политики безопасности в ИВС.

ЛИТЕРАТУРА

1. Указ Президента Республики Казахстан от 17 мая 2003 года № 1096 О Стратегии индустриально-инновационного развития Республики Казахстан на 2003-2015 годы.

2.Т.Хакимова . Инновационные методы обучения информатике(учебное пособие).**ISBN 9965-830-45-2.**

Научный руководитель:к.п.н.доцент Т.ХАКИМОВА