УДК 004.9

ПРОБЛЕМА БЕЗОПАСНОСТИ РАСПРЕДЕЛЁННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Ткаченко П.В., студент гр. ПИм-191, I курс
Научный руководитель: Крюкова В.В., к.т.н., доцент
Кузбасский государственный технический университет имени Т. Ф. Горбачева
г. Кемерово

С развитием информационных технологий человечество получило доступ к большим объемам и способам передачи данных. Созданная всемирная паутина, в которой находятся сотни миллионов пользователей, со временем превратилась в мир со своими законами и правилами. Устройства связанны между собой и кроме передачи и обработки информации, хранят огромные массивы различных баз данных.

Так, например, совокупность независимых компьютеров, которая представляется для их пользователей единым целым, является распределенной системой (РС). [1] Для них свойственна открытость, масштабируемость и прозрачность. В то же время, использование информации и ее хранение подразумевает соблюдение мер безопасности, которые защищают пользователей и их устройства от нанесения различного вреда.

Цель работы: исследовать угрозы безопасности и способы защиты РС на этапах создания и эксплуатации.

Уже на стадии создания любой системы, подразумевающей обмен данными, должна продумываться система безопасности. Выполняя ее разработку, специалисты сталкиваются с рядом проблем, которые необходимо решить:

- сложность структуры систем, зависящая от количества входящих в нее подсистем;
- различие их видов и функций, которые они выполняют;
- контроль за обеспечением доступа к ресурсам, которые находятся далеко друг от друга, зачастую в разных странах;
- большая вероятность того, что информационные ресурсы принадлежат различным владельцам.

Поэтому, если сравнивать с сосредоточенными сетями, одна из основных особенностей защиты информации в РС – это обеспечение гарантированной передачи данных по коммуникационной подсети.

Для распределенных информационных сетей характерно деление угроз на активные и пассивные. [2] Чтобы успешно им противостоять, системы безопасности должны проектироваться приспособленными к работе даже в случае выхода из строя отдельных подсистем. Для этого в РС предусматривают дуб-

лирующие маршруты для доставки сообщений. Предпринимают меры, препятствующие искажению и потере информации в каналах связи.

Первый вид угроз преследует цель получить наиболее полную информацию о системе путем прослушивания каналов связи. Активные угрозы оказывают непосредственное воздействие на передаваемые сообщения и могут провоцировать несанкционированную передачу данных по сети. В результате таких действий РС могут быть частично повреждены или полностью выведены из строя.

Для борьбы с возможными угрозами применяют разнообразные способы защиты. Используется шифрование каналов связи. Устанавливаются межсетевые экраны. А при многоуровневой защите предусматривают контроль доступа в помещения, введение методов одноразовых паролей для управления и идентификации при удаленном доступе.

В отдельности любое из указанных средств не способно гарантировать необходимого уровня информационной безопасности. Для решения поставленной задачи требуются комплексные методики защиты. Например, целесообразно рассмотреть следующий вариант. [3]

В первую очередь необходим детальный анализ вычислительных систем и сетей, защиту которых требуется организовать. Требуется проведение всесторонней оценки существующих вычислительных систем, включая взаимодействия между его элементами и имеющиеся уязвимости. Анализ должен проводиться специалистами в области IT-безопасности и администраторами систем. Практика показывает, что для развернутых, сложных по архитектуре систем невозможно на этапе проектирования и последующего внедрения избежать ошибок и неточностей.

Существующие технические средства тестирования позволяют в значительной степени автоматизировать процессы поиска уязвимостей, повышая эффективность и скорость работы. После сбора необходимой информации проводится ее оценка, по результатам которой выдвигаются предположения по существованию тех или иных уязвимостей системы. После этого проводится эмулирование атак с целью определения возможностей системы успешно им противостоять или подтверждения предположений о наличии в защите слабых мест.

При этом, чем больше уязвимостей выявлено и устранено, тем более эффективной окажется выстроенная система защиты. [4]

Следующим шагом выступает построение многоступенчатой защиты, включающей в себя программное обеспечение для выявления факторов внешнего вторжения в систему, средства сканирования вирусных кодов и так далее. Подобные программные продукты решают следующий набор задач:

- управление правами доступа пользователей и анализа работы с целью выявления факторов аномальной активности;
- мониторинг всех подключенных к системе устройств и установление настроек правил доступа пользователей;
- проведение анализа используемых кодов, как операционной системы,

так и устанавливаемых программ.

Следующим этапом следует создание систем предупреждения, оперативно передающих информацию о попытках несанкционированных действий. От решений подобного типа требуется обработка информация о происходящих атаках на элементы системы с максимально возможной скоростью предоставления данных. Использование типовых образцов вторжений и построение анализа на интеллектуальных принципах позволяет определять схожие по характеристикам инциденты.

Далее необходимо создание решений, позволяющих прогнозировать последующие действия нападающих, а также систем восстановления устойчивости систем к внешнему воздействию. Одновременно должны быть проработаны решения, позволяющие в условиях нападения сохранять работоспособность сети. [5] Среди возможных вариантов распространение получили:

- установление ограничений доступа для пользователей, вызывающих подозрение;
- применение дополнительных средств защиты, активируемых только при нападении;
- регулярное обновление программного обеспечения;
- использование изолированных сетей;
- информирование правоохранительных органов о фактах атак.

Однако обеспечить стопроцентную защиту компьютерных систем на сегодняшний момент невозможно. Тем не менее, благодаря методам и средствам защиты, которые предлагают современные технологии, можно существенно снизить риск нежелательного проникновения в информационную систему. В то же время необходимо принимать во внимание тот факт, что чем больше требуется обеспечить защищенность данных, тем больших затрат потребуется на обеспечение информационной безопасности. Как правило, затраты такого характера имеют склонность к постоянному росту, по причине развития научно-технического прогресса в области информационных технологий.

Список литературы:

1. Таненбаум Э., Ван Стеен М. Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 880 с.

2. Киреенко А.Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. – 2012. – №3. – С. 40-46.

3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр “Академия”, 2005. – 256 с.

4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Diasoft, 2001. – 688 стр.

5. Никишова, А.В. Нейросетевой анализ событий безопасности в информационной системе / А.В. Никишова, Р.Ф. Рудиков, Е.А. Калинина // Известия ЮФУ. Технические науки. – 2014. – №2. – С. 80-86.