ФАКТОРЫ, ВЛИЯЮЩИЕ НА ЗАЩИТУ ИНФОРМАЦИИ ПРИ ПРОЕКТИРОВАНИИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

Государственное учреждение
«Научно-исследовательский институт Вооруженных Сил Республики Беларусь»
г. Минск, Республика Беларусь

Яковцев П.А.

Утин Л. Л. – к-т техн. наук, доцент

Переход от единичных мэйнфреймов до корпоративных информационных сетей (КИС) позволило расширить возможности по информационному обмену внутри организации, повысить ее управляемость. Однако, с преимуществами, связанными с обработкой информации в КИС, появляются и сложности, связанные с защитой информации. Чем совершеннее, становятся информационные технологии - тем сложнее процесс обеспечения защиты информации. Учитывать эти вопросы целесообразно на этапе проектирования КИС.

В ходе анализа были выявлены основные факторы проектирования КИС, влияющие на защищенность информации:

1. Территориальный фактор.

Если раньше объектом защиты являлись отдельные компьютеры, по возможности объединённые в локально вычислительную сеть, то сейчас это совокупность разнесенных территориально сетей, которые имеют ряд особенностей:

увеличение зоны контроля (специалисту необходимо контролировать работу пользователей вне зоны его досягаемости);

в состав общей системы включаются комбинации различных аппаратно-программных средств (система настроенная на обеспечение безопасности информации может не сработать на удаленную систему, отсюда рост уязвимостей);

увеличение количества точек атаки (увеличение элементов КИС, а соответственно и промежуточных узлов передачи информации, каждый из которых является источником угрозы);

снижение контроля периметра (высокая расширяемость сетей ведет к тому, что становится сложно определить границы сети: один и тот же узел может быть доступен различным сетям);

снижение управляемости и контроля доступа к системе (возникает возможность атаки без получения физического доступа к определенному узлу).

2. Программный фактор.

Применение стороннего программного обеспечения, вызывает необходимость в:

выборе программного обеспечения (различное программное обеспечение, или даже различные версии одного и того же программного обеспечения, ведет к затруднению обеспечения безопасности КИС, так как у каждого программного продукта свой набор уязвимостей);

выборе средств защиты (отсутствие универсальных средств защиты, вынуждает организацию постоянно обновлять возможности средств защиты, вплоть до полной замены при модернизации программного обеспечения КИС, что вызывает рост расходов на систему информационной безопасности).

3. Организационный фактор.

Рост количества узлов КИС неизбежно вызовет необходимость в росте количества обслуживающего персонала, что вызовет **рост риска преднамеренных и непреднамеренных инсайдерских атак.**

4. Фактор принадлежности КИС.

Если КИС проектирует для себя коммерческая организация, то ее в первую очередь будет интересовать конфиденциальность информации циркулирующей в сети. В случае проектирования КИС для силовых структур их в «особый» период будет больше интересовать доступность информации.

5. Временной фактор.

При проектировании КИС организация заинтересована в как можно большем жизненном цикле создаваемой сети. При этом необходимо учитывать **длительную поддержку и сопровождение внедряемых средств защиты**;

6. Фактор кодирования.

При увеличении количества пользователей и плеча передачи информации растет роль средств криптозащиты.

7. Фактор управления.

В настоящее время особое внимание уделяется автоматизации управления существующими и перспективными средствами защиты, например путем введения АСУ защитой информации КИС.

8. Финансовый фактор.

Система защиты требует больших материальных затрат, в частности на:

программную составляющую КИС (новое ПО, поддержка старого ПО и т.д.);

техническую составляющую КИС (сетевое оборудование, серверы, постройка или аренда линий связи и т.д.);

организационную составляющую (найм или содержание штатных программистов, системных администраторов, проведение аудита безопасности и защищенности КИС и т.д.).

Таким образом, рассматривая вопросы создания КИС, специалистам следует учитывать вышеизложенные факторы, влияющие на ее безопасность.