АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Анищенко В.А.

Анищенко Виктор Александрович – студент магистратуры,
факультет прикладной математики и информатики,
Московский авиационный институт,
Учебный центр «Интеграция», г. Серпухов

Аннотация: *в статье рассмотрены основные угрозы и уязвимости информационной безопасности организации.*

Ключевые слова: *угрозы, злоумышленник, информационная безопасность.*

Для построения полноценной защиты для информационной инфраструктуры организации (ИИО) необходимо иметь полное представление обо всех реальных и потенциальных угрозах, которые могут иметь место в системе [1].

Все существующие современные угрозы для ИИО подразделяют на такие классы [2]:

- угроза целостности (повреждение, искажение, уничтожение информации);
- угроза конфиденциальности (любое нарушение конфиденциальности документа или информации);
- угроза работоспособности системы (умышленные хакерские атаки или ошибки пользователей);
- угрозы сбоя в ПО и оборудовании.

Важное значение при построении ИИО имеет упорядочение документооборота, что позволяет обеспечить намного более качественную систему защиты. При разработке защищенной среды электронного документооборота необходимо идентифицировать и проанализировать потенциальный круг источников угроз. Следует выделить основные группы источников угроз, в частности это: легальные пользователи системы, административный управляющий персонал и внешние/внутренние злоумышленники.

Согласно ряду исследований [3] до 80% потерь от подобных преступлений, по взлому корпоративных информационных систем, составляют атаки изнутри организации. Любой пользователь системы является потенциальным злоумышленником, в силу того, что он способен нарушить конфиденциальность информации, допустив ошибку или сделав осознанный выбор. Состав всех внешних злоумышленников отличается. Как правило, это конкуренты, реже партнеры, иногда в качестве злоумышленников выступают клиенты.

Любая защищенная ИИО обязана обеспечивать следующие средства защиты для выполнения главных функций по обеспечению:

- сохранности документов;
- безопасного доступа;
- конфиденциальности;
- подлинности документов;
- протоколирования всех выполняемых действий пользователей.

ИИО должна содержать функциональности по обеспечению сохранности хранящихся документов от порчи и потери, а также обладать возможностями быстрого восстановления. Современные методы защиты ИИО, применяемые на практике, включают в себя:

- аутентификация пользователей и разделение доступа;
- подтверждение авторства электронного документа;
- контроль целостности электронного документа;
- конфиденциальность электронного документа;
- обеспечение юридической значимости электронного документа;
- контроль целостности используемого программного обеспечения;
- регистрация событий в информационных системах;
- криптографическая защита;
- межсетевое экранирование;
- антивирусная защита;
- использование виртуальных частных сетей;
- аудит ИБ (периодический и по требованию).

Анализ специфики функционирования современных ИИО позволил определить такие возможности расположения злоумышленника [4]:

- злоумышленник находится непосредственно в сети всех зарегистрированных пользователей, что дает ему возможность получить доступ к Web-интерфейсу ИС, при этом он не обладает зарегистрированной учетной записью;
- злоумышленник имеет возможность получить доступ к Web-интерфейсу ИС, при этом он обладает всеми необходимыми правами зарегистрированного пользователя;
- злоумышленник расположен в изолированной сети;
- злоумышленник получил доступ администратора ИС;
- злоумышленник получил доступ к интерфейсу регистрации.

В соответствии с предполагаемыми типами атак могут быть определены возможные категории нарушителей:

- хакеры, преступные организации или конкуренты - N1;
- бывшие сотрудники организации - N2;
- лица, относящиеся к техническому персоналу, не обладающие доступом к ИИО, партнеры и клиенты - N3;
- пользователи, обладающими правами доступа к корпоративной ИС - N4;
- пользователь систем электронного документооборота (СЭД) - N5;
- администраторы модулей корпоративной ИС - N6;
- администратор СЭД - N7;
- администраторы ИБ - N8.

Данные роли нарушителей отличаются степенью осведомленности, уровнем технической подготовки, оснащенностью необходимым оборудованием, а также глубиной уровня, на котором они способны провести задуманную атаку. В рамках ИИО, как правило, устанавливаются такие функциональные уровни: физический, сетевой, уровень сетевых сервисов, уровень ОС, уровень БД ИС, уровень итогового пользователя.

Список литературы

1. *Акимов В.А.* Нечеткие модели в природе, техносфере, обществе и экономике / В.А. Акимов, В.В. Лесных, Н.Н. Раднаев. М.: Деловой экспресс, 2004. 352 с.
2. *Аронов И.З.* Современные проблемы безопасности технических систем и анализа риска / Аронов И.З. // Стандарты и качество, 1998. № 3. С. 451.
3. *Борисов В.В.* Нечеткие модели и сети. / В.В. Борисов, В.В. Круглов, А.С. Федулов, М.: Горячая линия-Телеком, 2007. 284 с.
4. *Симонов С.В*. Анализ рисков, управление рисками / С.В. Симонов. Jet Info, 2003. 28 с.