УДК 004.492.2

АНАЛИЗ МОДЕЛИ УГРОЗ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКИХ СИСТЕМАХ

Дудин А.А. студент; ПеретякаА.О. студент; Губенко Н.Е., доц.
(Донецкий национальный технический университет)

Различные типы общества сегодня сменяют друг друга с неукротимой скоростью. На смену постиндустриальному пришел информационный и креативный. И на главенствующее место труда и капитала пришла информация, требующая сегодня особой защищенности от атак нарушителей. Сегодня этой проблемой занимаются крупнейшие международные организации и государственные структуры. Актуальность работы заключается в анализе одного из методов обеспечения информационной безопасности.

В данной работе поставлена цель провести анализ модели угроз нарушителя в информационных системах банковских структур. [1]

Адекватные модели угроз информационной безопасности позволяют выявить существующие угрозы, разработать эффективные контрмеры, повысив тем самым уровень ИБ, и оптимизировать затраты на защиту.

Рисунок 1. Схема создания модели угроз ИБ.

В работе модель нарушителя формируется в результате анализа следующих этапов:

- определение источников угроз.
- выявление критических объектов информационной системы.
- определение перечня угроз для каждого критического объекта.
- выявление способов реализации угроз.
- оценка материального ущерба и других последствий возможной реализации угроз. [2]

Для того, чтобы модель нарушителя приносила максимальную пользу и была наиболее информативна, она должна быть сориентирована на конкретный объект защиты (модель не может быть универсальной), учитывать мотивы действий и социально-психологические аспекты нарушения, потенциальные возможности по доступу к информационным ресурсам различных категорий внешних и внутренних нарушителей на различных пространственно-временных срезах объекта защиты.

Модель определяет нарушителей ИБ банковских систем как субъектов, действия которых могут привести к нарушению безопасности информации. Они могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомых со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеющих возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

Следующим пунктом является определение критических объектов ИС.

Целями несанкционированных действий нарушителя, способных привести к совершению НСД к защищаемым ресурсам ИС и нарушению принятых для ИС характеристик информационной безопасности, являются:

- нарушение целостности защищаемых ресурсов;
- нарушение конфиденциальности защищаемых ресурсов;
- нарушение доступности защищаемых ресурсов;
- создание условий для последующего проведения атак.

Для внутреннего нарушителя это может быть сами каналы передачи информации, программно-аппаратные средства из состава ИС, каналы связи ИС, по которым осуществляется передача персональных данных.

Для внешнего нарушителя это будут визуально-оптические каналы, носители информации, оставленные за пределами контролируемой зоны, общедоступные каналы связи, по которым осуществляется передача информации ограниченного доступа.

Для ИС банковских систем актуальны следующие типовые угрозы:

1) угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ):

- угрозы, осуществляемые при непосредственном физическом доступе к ТС ИС:
- угрозы, осуществляемые с использованием протоколов межсетевого взаимодействия:

2) угрозы утечки по техническим каналам утечки информации:

- просмотр информации на дисплее лицами, не допущенными к обработке ПДн;

- просмотр информации на дисплее лицами, не допущенными к обработке ПДн с использованием технических (в т.ч. оптических) средств. [1]

В ходе написания статьи была проанализирована модель угроз нарушителя ИБ банковских систем и были сделаны следующие выводы. К достоинствам модели можно отнести полное и структурированное описание источника угроз в лице внутреннего и внешнего нарушителя. Описаны каналы, по которым могут проводиться атаки на информационную систему, и угрозы, связанные с этими каналами, однако, на наш взгляд, необходима более полная информация о способах реализации угроз по представленным каналам. В качестве источника дополнения модели предлагаем использовать статистическую информацию о несанкционированных проникновениях в информационные системы, полученную от предприятий банковской сферы.

Перечень ссылок

1.Ярочкин, В.И. Информационная сохранность. Учебник для студентов вузов / 3-е изд. - М.: Академический проект: Трикста, 2005.-544 с.

2.Барсуков, В.С. Современные технологии сохранности / В.С. Барсуков, В.В. Водолазский. - М.: Нолидж, 2000. - 496 с.