

Профиль и жизненный цикл угрозы

написано Александр Астахов | 10 июня, 2023

Формально угрозу можно описать, используя понятия *профиля* и *жизненного цикла угрозы*.

Профиль угрозы определяется следующими статическими атрибутами:

- *Название угрозы* (в соответствии с принятой классификацией).
- *Общее описание угрозы*.
- *Источник угрозы*, описываемый моделью нарушителя.
- *Вид угрозы* – указывает на принадлежность к тому или иному известному виду угроз согласно их классификации.
- *Способ реализации* – указывает на принадлежность к тому или иному известному способу реализации данного вида угрозы согласно их классификации.
- *Объект защиты* (виды активов, на которые направлена угроза).
- *Последствия* (результат) осуществления угрозы.
- *Уязвимости* (предпосылки возникновения угрозы, такие как наличие определенных изъянов защиты, нарушения технологического процесса проектирования и разработки ПО и т. п.).

Поскольку реализация любой угрозы представляет собой определенную последовательность действий и/или событий, то при описании угрозы, помимо профиля, описывающего статические характеристики угрозы, для описания ее динамических характеристик используется понятие *жизненного цикла угрозы*.

Этапы реализации большинства угроз безопасности (жизненный цикл угроз), включают в себя следующие процессы:

- зарождение;
- развитие;
- проникновение в АС;
- проникновение в критичную информацию;
- инициализация;
- результат действия;
- регенерация.

В качестве примера рассмотрим профиль угроз безопасности, связанных с получением внутренними злоумышленниками несанкционированного доступа (НСД) к информационным активам организации.

Профиль угрозы:

- название угрозы – НСД к информации;
- общее описание угрозы – пользователь может получить доступ к ресурсам АС или выполнить операции, на которые ему не было предоставлено соответствующих прав;
- источник угрозы – можно выделить следующие категории потенциальных нарушителей:
 - операторы, обладающие самым низким уровнем возможностей, предоставляемых им штатными средствами АС, – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации;
 - прикладные программисты, которым предоставляется возможность создания и запуска собственных программ с новыми функциями по обработке информации;
 - администраторы АС и системные программисты, которым предоставляется возможность управления функционированием АС, т. е. воздействия на базовое программное обеспечение системы, а также состав и конфигурацию ее оборудования;
- разработчики АС и лица, обладающие всем объемом

возможностей по проектированию, реализации и ремонту технических средств АС, вплоть до включения в ее состав собственных технических средств по обработке информации;

- вид угрозы – использование штатных средств для осуществления НСД к информации АС;
- способ реализации – подбор или воровство пароля, использование слабостей защиты;
- объект защиты – база данных;
- последствия – утечка конфиденциальной информации из базы данных;
- уязвимости – ошибка в настройке правил разграничения доступа к базе данных, нарушение сотрудниками правил парольной политики, уязвимости программного обеспечения базы данных или операционной системы.

Жизненный цикл угрозы:

- зарождение – возникновение предпосылок для НСД;
- развитие – выявление возможностей и способов НСД к информационным ресурсам АС;
- проникновение в АС – НСД к ресурсам АС при помощи штатных средств;
- проникновение в критичную информацию – путем обхода средств разграничения доступа;
- инициализация – копирование конфиденциальной информации;
- результат действия – в соответствии с целями НСД;
- регенерация – при повторном НСД.

Описанная группа угроз включает в себя множество угроз, предполагающих различные сценарии развития инцидентов, различные виды нарушителей и используемых ими уязвимостей.

Следует ли при разработке модели угроз отдельно описывать подгруппы угроз и отдельные угрозы входящие в группу, зависит

от конкретной ситуации с рисками и потребностей организации. Основным критерием здесь служит достаточность информации, предоставляемой по результатам процесса оценки рисков, для принятия руководством организации обоснованных решений по обработке рисков. Например, при рассмотрении чрезвычайных ситуаций, приводящих к потере оборудования и помещений, угрозу пожара не следует объединять в одну группу с угрозами наводнения, землетрясения или урагана, т.к., несмотря на общие последствия этих угроз и их случайный характер, они существенно отличаются по вероятности, используемым уязвимостям и механизмам контроля, необходимым для их уменьшения.

Разработка профилей угроз является полезным упражнением для эксперта по оценке рисков. Эта задача требует определенного навыка. Далее мы рассмотрим различные виды и классификации угроз безопасности более подробно. Однако, прежде чем переходить к следующим разделам, рекомендуем вам самостоятельно выполнить Задание №1.