Рысенкин О.В. Анализ моделей нарушителей для Интернет-технологий. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей VIII Всерос. научно-техн. конф. – Пенза: ПДЗ, 2008. – С. 113-115.

АНАЛИЗ МОДЕЛЕЙ НАРУШИТЕЛЕЙ ДЛЯ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

О.В. Рысенкин

Астраханский государственный технический университет,
г. Астрахань

Нарушитель – это лицо, которое предприняло попытку выполнения запрещенных операций по ошибке, незнанию или осознанно, со злым умыслом или без такового и использующее для этого различные методы и средства.

Всех нарушителей с учетом категории лиц, мотивации, наличия специальных средств, доступа к информационной системе Интернет-провайдера (ИСП) можно разделить на внутренних и внешних.

Внутренние нарушители:

1. «Невнимательный пользователь» выполняет запрещенные операции доступа к ресурсам ИСП с превышением своих полномочий. Действует по ошибке без злого умысла на своем рабочем месте (РМ).

2. «Сотрудник-нарушитель» преодолевает защиту для самоутверждения. Использует методы получения дополнительных полномочий доступа к ИСП, в выделенные помещения (ВП), недостатки в построении защиты, нештатные программы.

3. «Сотрудник-злоумышленник» действует целенаправленно, в сговоре с другими лицами вследствие подкупа конкурентами. Изменяет счета, финансовые отчеты, вводит подложные данные в ИСП. Использует весь набор пассивных и активных методов и технических средств (ТС) воздействия.

Аналогично разделяем и внешних нарушителей на следующие группы:

1. «Хакер-любитель» для которого проникновение в систему является головоломкой, работой для ума. Хакер повышает свое мастерство.

2. «Профессиональный хакер» ищет известности, славы и признания. Может быть уволенным сотрудником, знающим слабости системы. Его действия обычно направлены на конкретного провайдера.

3. «Внешний злоумышленник» действует целенаправленно в сговоре с другими лицами. Использует весь набор технических способов нарушения безопасности, характерных для сетей общего пользования. Финансовая выгода – мотив как для отдельных хакеров, так и для компаний-конкурентов.

Необходимо оценить степень опасности категории нарушителя определенному элементу системы, времени и места воздействия и представить результаты анализа в виде таблицы.

Критерии оценки рисков следующие: фатальная опасность – **4**; повышенная опасность – **3**; средняя опасность – **2**; низкая опасность – **1**; нет угроз – **0.**

Элементы ИСП: **I** – внутренние данные; **II** – внутренние модули; **III** – внешние данные, информация, расположенная на серверах компании; **IV** – внешние системные модули, система авторизации, внешние сервера.

Степень опасности различных категорий нарушителей

Категории нарушителей	***Элементы ИСП***												***Время воздействия***	***Место воздействия***
	I			***II***			***III***			***IV***				
	Виды ущерба													
	А	*Б*	*В*	*А*	*Б*	*В*	*А*	*Б*	*В*	*А*	*Б*	*В*		
Неопытный	2	1	2	2	1	2	2	1	3	2	2	2	*При работе ИСП*	*РМ сотрудника*
Сотрудник-нарушитель	1	2	4	3	2	3	3	1	4	1	1	2	*При работе ИСП и в перерывах*	*Со своего АРМ, в ВП без доступа к ТС*
Сотрудник-злоумышленник	4	3	4	4	3	3	4	4	4	3	2	3	*В моменты пиковых нагрузок ИСП, в нерабочее время*	*В ВП с доступом к ТС, в зоне управления средствами безопасности*
Хакер-любитель	0	0	1	1	0	0	0	1	0	3	2	3	*При работе ИСП*	*Из-за пределов контролируемой зоны (КЗ), из сети Интернет*
Профессиональный хакер	1	0	2	0	0	0	1	1	2	3	2	4	*Сканирование ИСП при работе, атака при обнаружении уязвимостей*	*Из-за пределов КЗ, из сети Интернет, с маскировкой места атаки*
Внешний злоумышленник	3	2	4	3	3	4	2	1	3	4	4	4	*Атака при обнаружении уязвимостей и при максимальных нагрузках, в перерывы для технического обслуживания и ремонта*	*Из-за пределов КЗ, из сети Интернет, в ВП при проведении технических работ, с доступом к ТС*

Виды ущерба: **А** – модификация, изменение, искажение, нарушение целостности данных, технических средств обработки информации в ИСП; **Б** –

разрушение, уничтожение данных и программно-аппаратных средств ИСП; **В** – раскрытие информации, составляющей коммерческую и служебную тайну.

Анализ моделей нарушителей просто необходим при разработке политики безопасности (ПБ) любого Интернет-провайдера. Необходимо по полученным критериям опасности различных нарушителей избирательно разрабатывать методы и средства защиты.

Полученная таблица критериев может быть автоматизирована, для того чтобы различные эксперты для различных компаний-заказчиков по полученным критериям могли делать оценки, результаты которых лягут в основу построения ПБ реального оператора связи.