III НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИКИ, СВЯЗИ И ИНФОРМАТИКИ

УДК 621.38

МОДЕЛЬ ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ ДИСТАНЦИИ СИГНАЛИЗАЦИИ И СВЯЗИ

К. А. БОЧКОВ, П. М. БУЙ, М. В. ЛУКАШЕНЯ
Белорусский государственный университет транспорта, г. Гомель

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. п. Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности.

К внутренним нарушителям информационной безопасности системы обычно относят следующие категории субъектов: 1) непосредственные пользователи и операторы информационной системы, в том числе руководители различных уровней; 2) администраторы вычислительных сетей и информационной безопасности; 3) прикладные и системные программисты; 4) сотрудники службы безопасности; 5) технический персонал по обслуживанию зданий и вычислительной техники, от уборщицы до сервисного инженера; 6) вспомогательный персонал и временные работники.

Для анализа среди сотрудников дистанции сигнализации и связи были выделены следующие группы субъектов: 1) руководители; 2) основной персонал; 3) вспомогательный персонал; 4) технический персонал. В таблице 1 показано распределение субъектов дистанции сигнализации и связи по группам.

Согласно [1], основными причинами, побуждающими сотрудников к неправомерным действиям, являются: злой умысел (демонстрация своего превосходства, «борьба с системой»; корыстные интересы); ошибки пользователей или администраторов; безответственность; (самоутверждение); ошибки программного обеспечения (ПО) и аппаратных средств.

Таблица 1 – **Распределение сотрудников по группам**

Субъект (должность)	Группа	Субъект (должность)	Группа
Агент по снабжению	2	Кладовщик	3
Бухгалтер	2	Начальник участка КТСМ	1
Главный бухгалтер	1	Начальник участка связи	1
Главный инжинер	1	Секретарь	3
Диспетчер ШЧ	1	Старший диспетчер ШЧ	1
Зам. начальника по кадрам	1	ШН КИПа связи	1
Зам. начальника по связи	1	ШН техдокументации	2
Зам. начальника по СМБ	1	ШНС КИПа АБ	2
Инженер по надежности	2	ШНС КИПа связи	1
Инженер по охране труда	2	ШНС техдокументации СЦБ	2
Инженер технического отдела	4	Экономист	2
Инспектор по кадрам	2		

В таблице 2 для групп субъектов, ставших по тем или иным причинам нарушителями информационной безопасности, представлены основные причины их действий, методы, средства, уровень их знаний и время воздействия. Знаком «+» обозначены те свойства, которые присущи той или иной группе субъектов.

Таблица 2 – **Модель нарушителя информационной безопасности**

		Группа субъектов			
		1	2	3	4
Причина		+	+	+	+
	Злой умысел	+	+	+	+
	Неопытность (ошибка)	+	+	+	+
	Безответственность	+	+	+	+
	Ошибки ПО и аппаратных средств	+	+	+	+
Методы и средства	Сбор информации и данных	+	+		+
	Использование средств, входящих в информационную систему или систему информационной безопасности, и их недостатков	+			+
	Подключение новых средств, использование специализированных утилит, внедрение программных закладок в систему	+			+
	Подключение к каналам скрытого удаленного управления				+
Уровень знаний	Максимальный	+			+
	Достаточно большой	+	+	+	+
	Недостаточно большой		+	+	
	Минимальный	+	+	+	+
Время воздействия	В процессе выполнения должностных обязанностей	+			+
	В прочее время				

В таблице 3 показаны потенциальные действия сотрудников дистанции сигнализации и связи, ставящие их на место нарушителей информационной безопаснсоти. Знаком «+» отмечены те группы субъектов, которые могут умышленно или нет произвести угрозу.

Таблица 3 – **Действия сотрудников дистанции сигнализации и связи**

Действия сотрудников дистанции сигнализации и связи	Группа субъектов			
	1	2	3	4
Ошибки при разработке алгоритмов и ПО				+
Ошибки при инсталляции и загрузке ПО	+	+	+	+
Ошибки при эксплуатации ПО	+	+	+	+
Ошибки при вводе данных (информации)	+	+		+
Повреждение (удаление) ПО	+	+		+
Повреждение (удаление) данных	+	+		+
Нарушение соблюдения конфиденциальности	+	+	+	+
Нарушение энергообеспечения технических средств и ПО				+
Нарушение жизнеобеспечения технических средств и ПО				+
Установка нештатного оборудования				+
Инсталляция нештатного ПО (игрового, обучающего, технологического)	+	+	+	+
Нарушение правил обработки и обмена информацией	+	+		+
Нарушение хранения и повреждение (уничтожение) носителей информации	+			+
Повреждение каналов связи	+	+	+	+
Ошибки при настройке сервисов универсальных систем				+
Ошибки при включении/выключении технических средств	+	+	+	+
Ошибки при конфигурировании и управлении сложной системы				+
Ошибки при настройке ПО				+
Ошибки при организации управления потоками обмена информации	+			+
Ошибки при настройке технических средств				+
Ошибки при настройке штатных средств защиты ПО				+

Очевидно, что сотрудники с большими полномочиями и доступом к информационной системе имеют больше возможностей оказаться на месте нарушителей информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1 **Теренин, А. А.** Как построить модель типового нарушителя информационной безопасности / А. А. Теренин // Защита информации. INSIDE,– 2005. – № 5. – С. 18–24.