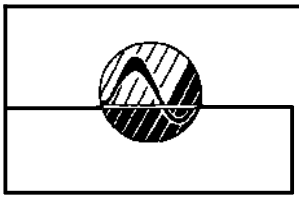

ПОВІДОМЛЕННЯ

УДК 004.056.53

К ВОПРОСУ ИССЛЕДОВАНИЯ ВНУТРЕННИХ УГРОЗ

Е.С. Клименко
(Ставропольский государственный университет, Ставрополь, Россия)

В работе рассмотрены наиболее опасные внутренние угрозы, источники возникновения внутренних угроз, разделение внутренних угроз по способу нанесения ущерба. Приведена вербальная модель парирования внутренним угрозам.

внутренние угрозы, источники возникновения, разделение по способу нанесения ущерба, вербальная модель, парирование внутренних угроз

Результаты исследований многих авторитетных аналитических организаций выявили актуальность проблемы внутренних угроз (ВУ) безопасности [1].

Действия сотрудников представляют наибольшую опасность. Наиболее опасные ВУ [1]: утрата информации – 7 %; кража оборудования – 6%; сбои в работе информационных систем – 15 %; искажение информации – 62 %; нарушение конфиденциальности информации – 98 %; другое – 28 %.

По данным Ernst&Young [2], человеческий фактор занимает первое место в списке обстоятельств, препятствующих проведению эффективной политики ИТ-безопасности. Исследования InfoWatch [1], Ernst&Young [2], Association of Certified Fraud Examiners [3] свидетельствуют об опасности, которую представляют сотрудники. Высок уровень латентности преступлений, связанных с выше перечисленными внутренними угрозами, в США – 80%, в Великобритании – 85%, в ФРГ – 75%, в России – более 90% [1, 2].

Источниками ВУ могут быть: администрация предприятия; персонал; технические средства обеспечения производственной и трудовой деятельности.

По способу нанесения ущерба ВУ можно подразделить [1]:

– неавторизованный доступ в систему;

– неавторизованный поиск/просмотр конфиденциальных данных;

– неавторизованное изменение, уничтожение, манипуляции или отказ доступа к информации, принадлежащей компьютерной системе;

– сохранение/обработка конфиденциальной информации в системе, не предназначенной для этого;

– попытки обойти/взломать систему безопасности или аудита без авторизации системного администратора;

– другие нарушения процедур и правил внутренней безопасности сети.

Проблема утечки информации через персонал является частью проблемы информационной безопасности организации. Ее решение эффективно в комплексе организационных и процедурных мероприятий по защите информации, поддерживаемом единым комплексом программно-технических средств защиты [4]. В связи с этим возможна следующая модель парирования внутренним угрозам безопасности [5]:

– организационные методы (ориентация на работу с персоналом, тренинги сотрудников);

– инженерно-технические методы (построение оптимальных сетей инженерных коммуникаций, например, построение системы физического доступа);

– технические методы (технические средства защиты информации и контроля обстановки, например, системы мониторинга электронной почты, Internet-трафик, комплексные системы мониторинга сетевых ресурсов [6]);

– программно-аппаратные методы (устранение угроз – с процессом обработки и передачи информации, например, ограничение связи с внешними сетями).

Все группы должны иметь равную долю в организации комплексной защиты.

Таким образом, в организации должны соблюдаться технические, образовательные и нормативные меры.

Технические меры должны быть соблюдены с учетом «Специальных требований и рекомендаций по технической защите конфиденциальной информации» [7].

Образовательные меры включают обучение пользователей основам информационной безопасности. Необходимо внедрение системы мониторинга действий сотрудников. [6]

Нормативные меры – проведение тренингов персонала, создание документов, описывающих политику обращения с электронной конфиденциальной информацией. Политика должна описывать виды информации, присваивать категорию ее конфиденциальности и определять правила работы с ней [8].

Необходимо вести учет всех возможных внутренних атак и путей утечки информации, контроль операций с данными внутри сети в соответствии с политикой безопасности организации, не допустить разрыва между политикой организации в области информационной безопасности и реальной практикой функционирования средств защиты [9].

Цена утечки информации возрастает пропорционально росту числа сотрудников организации. Необходимо четко представлять масштабы ВУ. На данный момент существует разрыв между оценкой критичности внутренних угроз и практическими шагами по ее нейтрализации. Утечка информации – необратимый процесс, поэтому ошибка в защите конфиденциальной информации практически неустранима, поэтому целесообразно создание эффективной [10] комплексной системы защиты информации от внутренних угроз.

ЛИТЕРАТУРА

1. *Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) // Решение Коллегии Гостехкомиссии России № 7.2/02.03.01*
2. *Ernst & Young Global Information Security Survey 2004. – [Электр. ресурс]. – Режим доступа: www.ey.com*
3. *Внутренние ИТ-угрозы в России 2004 // Исследование компании Info-Watch.– [Электр. ресурс]. – Режим доступа: www.infowatch.ru*
4. *Association of Certified Fraud Examiners.– [Электр. ресурс]. – Режим доступа: www.cfenet.com.*
5. *Ляпунов И. Информационная безопасность и персонал // Безопасность и персонал. – 2002. – № 3. – С. 32 – 39.*
6. *Клименко Е.С., Росенко А.П. Мониторинг безопасности корпоративной сети с учетом проявления внутренних угроз информации ограниченного распространения // Сб. тез. 12 Общерос. НТК «Методы и технические средства обеспечения безопасности информации», 4-5 октября 2004. – С.-Пб.: СПГПУ. – 2004.*
7. *Соколов А.В., Вихорев С.В. Как оценить угрозы безопасности информации // Технологии и средства связи. – 2000. – № 5.*
8. *Офисные предатели опаснее хакеров. – [Электр. ресурс]. – Режим доступа: www.server.md.*
9. *Гриняев С.Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 224 с.*
10. *Росенко А.П., Клименко Е.С. О выборе критерия оценки эффективности функционирования систем защиты информации // Сб. тез. Первой заочной международной НТК «Инфотелекоммуникационные технологии в науке, производстве и образовании», 19 декабря 2004. – Ставрополь: СКГТУ, 2004. – С. 207 – 208.*

Поступило 25.05.2005