С. В. КАВУН, С. П. ЕВСЕЕВ, И. В. СОРБАТ,
Харьковский национальный экономический университет

МОДЕЛЬ РАБОТЫ ИНСАЙДЕРОВ НА ПРЕДПРИЯТИИ

In the article new procedures of bucking insiders at enterprise which it is planned to use for construction of new model of work insiders at enterprise on the basis of standard IDEF0 are offered. For protection of transmission channels of the information new algorithms of crypting are offered. The comparative analysis of the statistical data received during probing is resulted also.

Сегодня в современном мире, в эпоху стремительного развития ИТ-технологий и их внедрения в экономику предприятия, особенно актуальным становится вопрос обеспечения экономической безопасности (ЭБ) предприятия при нежелательных (незаконных) действиях своих сотрудников. Одной из таковых категорий являются **инсайдеры**.

Целью статьи является показ возможных схем реализации действий инсайдеров для руководителей различных рангов и построение плановых мероприятий по устранению каналов утечки категорированной информации на предприятии. **Объектом исследования** является система ЭБ предприятия, построенная на базе различных моделей управления, например, представленной в работе [1].

Проведенный сравнительный анализ источников статистической информации (Computer Security Institute, CSI, [2]) показал устойчивую тенденцию роста уровня потерь различных ресурсов предприятия от деятельности инсайдеров. Свидетельством тому является показатель превышения уровня инцидентов в 2007 году на предприятиях, связанных с инсайдерами, по сравнению с вирусными заражениями.

Предотавлено множество возможных вариантов деятельности инсайдера, где общее их количество составляет 16 с учетом всех комбинаций.

Дальнейшие организационные меры по выявлению (предотвращению деятельности) и ликвидации последствий являются базовыми и могут выглядеть следующим образом:

1. Усиление правил использования и составления паролей.
2. Внедрение и тщательное соблюдение известных (мировых) стандартов, внутренних инструкций, законодательных актов, норм, правил, законов.
3. Четкое разграничение прав доступа и внимательный выбор объекта для делегирования текущих прав другим сотрудникам.
4. Введение на предприятии собственной службы информационной и экономической безопасности, а также группы улаживания инцидентов по компьютерной (информационной и экономической) безопасности – ГУИКБ [4].
5. Плановое (еженедельное, квартальное, полугодовое, годовое, внеплановое) обследование предприятия на предмет выявления известных (и не известных) каналов утечки информации.
6. Использование системы масштабного "логирования" (записи в файл всех операций, действий, транзакций) для наиболее уязвимых мест системы и критичных ресурсов предприятия.

Экономическая модель работы инсайдеров на предприятии. Все инсайдеры работают по одним и тем же алгоритмам, отличие может зависеть только от специфики самого предприятия.

Схема работы инсайдера на предприятии представлена в графическом виде.

На основе разработанной схемы работы инсайдера получена модель функционирования в стандарте IDEF0 с ее декомпозицией.

Все модели в стандарте IDEF0 представлены для определения последовательности и взаимосвязи работ между собой без учета их стоимости.

При расчете утечек всегда учитывают внутренние и внешние потери, у 2% опрошенных предприятий общий ущерб превысил 5 млн. долларов. Выводом данного исследования может быть выделение наиболее чувствительных к финансовым потерям предприятий, среди которых на первом месте находятся банки, страховые компании, корпорации, холдинги, предприятия с зарубежной долей инвестиций.

Таким образом, зная виды деятельности или классификацию видов деятельности инсайдеров, можно разработать комплекс мероприятий (методику), направленный на

предотвращение или устранение последствий результатов их деятельности. В качестве основных видов деятельности разработаны ключевые аспекты методики противоборства с инсайдерами: предотвращение, выявление, ликвидация последствий.

В вышепредложенной методике на стадии *предотвращения* необходимо реализовывать защиту каналов передачи информации (категорированной: коммерческой, банковской, персональной, служебной, финансовой, аутентификационной). Здесь, например, можно применять криптографическое преобразование информации в кодовых криптосистемах на эллиптических кодах для каналов с автоматическим переспросом.

Эффективным механизмом комплексного повышения безопасности и достоверности информации являются кодовые криптосистемы [6-9]. Их использование позволяет обеспечить защиту информации от несанкционированного доступа и воздействия случайных ошибок. В то же время известные кодовые криптосистемы функционируют в режиме прямого исправления ошибок и не предполагают использования в каналах с автоматическим переспросом.

Для решения подобных задач предложены алгоритмы криптографического преобразования информации для каналов с автоматическим переспросом с использованием кодовых криптосистем на эллиптических кодах.

Использование данных алгоритмов, позволит выполнять задачу обмена секретными сообщениями между абонентами информационного обмена с использованием кодовых криптосистем на эллиптических кодах в каналах с автоматическим переспросом.

Таким образом, проблема внутренней ЭБ предприятия должна занимать достойное место в плане развития предприятия и получать все необходимые ресурсы (человеческие, организационные, финансовые и др.) для внедрения, реализации и соблюдения требований системы ЭБ предприятия.

Литература:

1. Кавун С. В. *Концептуальная модель системы экономической безопасности предприятия. Науковий журнал "Економіка розвитку"*. Харків, Вид. ХНЕУ. № 3(43). – Х.: 2007. – С.97-101.
2. FBI: *Computer Crime Survey [Электрон. ресурс]*: www.fbi.gov/publications/.
3. Кавун С.В. *Информационная безопасность в бизнесе*. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с.
4. Кавун С. В., Шубина Г. В. *Методика построения политики безопасности организации*. Научный информационный журнал "Бизнес Информ". ХНЭУ. № 1-2 – Х.: 2005. – С.96-102.
5. Криминальный кодекс Украины.
6. R.J. McEliece. *A Public-Key Criptosystem Based on Algebraic Theory*. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January-February, 1978. – P.114-116.
7. H. Niederreiter. *Knapsack-Type Cryptosystems and Algebraic Coding Theory*. // Probl. Control and Inform. Theoty. – 1986. –V.15. – P.19-34.
8. Стасев Ю.В., *Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов*. // Кибернетика и системный анализ: Международный научно-теоретический журнал. – Киев: НАНУ. – 2005. – №3. – С.47-57.
9. Евсеев С.П. *Несимметричный алгоритм шифрования с использованием эллиптических кодов*. // Проблеми інформатики і моделювання. Матеріали четвертої міжнародної науково-технічної конференції. – Х.: НТУ „ХПІ". – 2004. – С.12.