УДК 004.056.5

Сычев Е.В., Ищенко Ю.В.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

В настоящее время в системах, обеспечивающих экономическую безопасность предприятий, разрабатываются и применяются различные инструменты управления информацией, включая современную технику и оборудование, программное обеспечение и документацию, технологии искусственного интеллекта и автоматизированные ресурсы для управления потоками информации в открытых и закрытых сетях. Методы управления информационными технологиями разрабатываются в системах, обеспечивающих экономическую безопасность предприятий. Об этом свидетельствует тот факт, что они адаптируются к процессу управления информацией и обеспечивают экономическую безопасность в связи с использованием современных систем информационных технологий [1].

Информационная безопасность обеспечивает защиту данных от кражи или изменений, например случайного или преднамеренного характера. Системы, которые обеспечивают безопасность информации вашей организации, являются эффективным инструментом защиты интересов владельцев информации и пользователей. Следует отметить, что ущерб может быть причинен не только несанкционированным доступом к информации.

Чтобы обеспечить надлежащую защиту информации, необходимо иметь четкое представление об основах, целях и роли информационной безопасности [2].

Для обеспечения защиты информации используются следующие методы:

1) **Препятствие**. Метод представляет собой использование физической силы с целью защиты информации от преступных действий злоумышленников с помощью запрета на доступ к информационным носителям и аппаратуре.

2) **Управление доступом** – метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям.

3) **Маскировка** – метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе.

4) **Регламентация** – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму.

5) **Принуждение** – это метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.

6) **Побуждение** – метод, который основан на этических и моральных нормах, накладывающих запрет на использование запрещенной информации, и побуждает соблюдать установленные правила. Все перечисленные методы защиты направленны на обеспечение максимальной безопасности всей информационной системы организации и осуществляются с помощью разных защитных механизмов. Для достижения качественного и разумного управления информацией в системах, обеспечивающих экономическую безопасность, компании должны использовать широкий спектр инструментов, важную роль в которых играют современные информационные технологии [3].

Кроме того, для повышения экономической безопасности компании можно использовать различные информационные продукты. Чаще всего это численное выражение состояния той или иной составляющей экономической безопасности. Для проведения расчетов результаты должны быть объяснены, чтобы принять дальнейшие решения по улучшению существующих параметров, которые влияют на систему для обеспечения экономической безопасности предприятий.

Список использованных источников

1. Корчевская Л.О. Итеративный подход к исследованию экономической безопасности предприятия. / Л.О. Корчевская - №4, - 2012. - 111-119. с.

2. Филиппова С.В. Система формирования и обеспечения экономической безопасности предприятия. / С.В. Филиппова, О.С. Дашковский. Научный журнал. - 2012. - №2 (3). - 17-21 с.

3. Кияев В. Безопасность информационных систем / В. Кияев, О. Граничин. - 2016. - 192 с.