МД ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ЗАО

PHANTOM

Современные технические средства на страже информационной безопасности

Сегодня ни у кого не вызывает сомнений, что информационная безопасность является одним из основных элементов организационного менеджмента. От эффективной защиты информации зависит успех практически всех направлений деловой активности предприятия и любого бизнеса в целом.

Под понятием "информационная безопасность" подразумевается создание комплекса мер по предотвращению возможных угроз деятельности организации.

Исходными условиями создания полноценной системы информационной безопасности должно быть четкое представление о самой ее сущности, структуре целей обеспечения безопасности, вытекающих из этих целей практических задачах, видах угроз и их источниках, а также о мерах противодействия.

Среди внутренних угроз безопасности несложно выделить наиболее типичные ее виды:

- разглашение конфиденциальной информации;
- хищение денежных средств;
- хищение собственности (интеллектуальной и имущества);
- фальсификация документов;
- использование собственности, средств и сил сотрудников предприятия не по назначению;
- профессиональная некомпетентность.

Важнейшим из этого перечня стоит считать вопрос защиты информации, которая может быть разделена на два самостоятельных блока информационных ресурсов:

- сведения, относящиеся непосредственно к самой организации;
- конфиденциальные сведения о поставщиках, клиентах и партнерах.

Плата за утечку любого типа конфиденциальной информации велика и даже при благополучном исходе способна обернуться существенной недополученной прибылью. А ведь вероятны и другие сценарии.

Меры по предотвращению утечки информации

Решение проблемы безопасности распадается на организацию решений ее отдельных элементов, где необходимым условием является обеспечение защищенности информации, циркулирующей внутри организации.

Изучение механизма движения информации в компаниях разного профиля показало необходимость разработки ряда процедур при работе с информацией, в частности:

- определение порядка допуска к работе над конфиденциальными источниками с дифференциацией информации на категории – "ДСП" (для служебного пользования), "К" (конфиденциальная) и "СК" (строго конфиденциальная) – и присвоением категорий допуска сотрудникам.
- внедрение системы документооборота и учета, обеспечивающей защиту информации от несанкционированного распространения между внутренними подразделениями;
- организационно-техническое разделение соответствующих подразделений, в частности, ограничение доступа к электронным базам данных с целью создания единой системы ограничения доступа к информации различного уровня для каждого сотрудника (например, открытие пользовательских директорий и предоставление каждому пользователю доступа к личной директории, куда переносятся все файлы, содержащие банковскую и личную информацию);
- закрепление требований к сотрудникам по сохранению информационной тайны и неразглашению конфиденциальной информации, например, через трудовой контракт;
- обеспечение технической базы для локализации источников утечки информации, в частности, использование оборудования для регистрации телефонных и прочих переговоров персонала.

Внутрифирменный контроль

Эффективность любой системы безопасности во многом зависит от соблюдения или игнорирования установленных организацией правил защиты информации.

Задача отслеживания исполнения принятых норм ложится на плечи службы безопасности или службы информационной защиты организации, в чьи основные функции входит проведение непроцессуального (внутреннего) расследования по фактам нанесения ущерба собственности и порядку функционирования организации.

Благодаря оснащению предприятия средствами автоматической регистрации данных удается выявлять нарушения, локализовывать источники и даже предупреждать утечку конфиденциальной информации при небольших людских и временных затратах.

Особое внимание следует уделить регистрации данных, передаваемых по слаботочным информационным сетям – телефонным линиям и ЛВС, пронизывающим компанию изнутри и связывающим ее с внешним миром.

Регистрация данных, передаваемых по ЛВС осуществляется, как правило, программными средствами и чаще всего не требует специальной аппаратной части, в то время как для записи и мониторинга переговоров требуется голосовая плата и специализированное программное обеспечение.

Примером оборудования для регистрации телефонных переговоров могут служить многоканальные системы мониторинга и регистрации переговоров семейства "Фантом". Цифровые регистраторы способны автоматически вести запись всех необходимых переговоров внутри организации и позволяют при необходимости осуществлять мониторинг в режиме реального времени.

Для проведения мероприятий по регистрации речевых сообщений необходимо придать гласность этому процессу. Для этого, например, можно назначить линии для ведения служебных переговоров и поставить в известность об этом сотрудников. Таким образом, проводимые по данным линиям переговоры считаются служебными. С другой стороны, необходимо сообщить клиентам организации о ведущейся записи речевых сообщений.

Соответствие множественным целям организации

Многоканальные регистраторы типа "Фантом" служат для решения таких задач, как:

- подключение к любому количеству и типу каналов связи;
- автоматическое ведение записи разговора и создание базы данных записей;
- регистрация всех параметров сеанса связи – АОН, дата, время, продолжительность разговора и т.д.
- быстрое нахождение нужной записи по заданным критериям;
- воспроизведение записи в разных скоростных режимах;
- создание внешнего архива.

Имея сходные параметры, системы "Фантом" по сравнению с зарубежными аналогами отличаются существенно более низкой стоимостью.

Системы записи не относятся к категории специальных технических средств. Оборудование семейства "Фантом" может использоваться для внутрифирменного контроля на основании положения "Об использовании систем мониторинга и записи "Фантом" в организациях".

МД ИНФОРМАЦИОННЫЕ СИСТЕМЫ

115280 Москва, ул. Автозаводская, 19, корп. 2
Тел.: (095) 274-6082
Факс: (095) 275-6082
E-mail: md@mdis.ru
www.mdis.ru