
В связи с участившимися взломами информационных баз данных, которые вредят работе различных предприятий, фирм, корпораций и даже приводят к их полному уничтожению, возникает важный вопрос о защите конфиденциальной информации. А для того, чтобы защита была надёжной, нужно понять и найти причины утечки закрытой информации. В этом ключе большинство специалистов, которые работают в сфере безопасности информационных систем, считают, что основное внимание нужно обращать на персонал предприятия, работающего с конфиденциальными сведениями.  Выделяют две главные задачи:

1) предельно усложнить работу злоумышленнику в целях получения нужной информации;

2) предотвратить установление каких-либо связей между злоумышленником и сотрудником фирмы, который владеет секретными данными.

Персонал предприятия может быть источником различных угроз в работе с конфиденциальной информацией. Способы осуществления угроз информационной безопасности предприятия могут быть различны. Сотрудник фирмы может действовать целенаправленно или неосознанно по собственной инициативе, а также под чьим-то влиянием.

Требования по работе с сотрудниками, имеющими доступ к конфиденциальной информации:

• обучение и постоянный инструктаж персонала;

• постоянное проведение воспитательной работы с сотрудниками, работающими с секретными данными;

• регулярный контроль работников за исполнением требований, связанных с защитой конфиденциальных данных;

• проверка углублённости знаний сотрудников в области засекреченной информации фирмы;

• осуществление служебных расследований в связи с утечкой секретных данных и нарушениями сотрудниками требований по защите информационной безопасности;

• усовершенствование методов обучения персонала.

Обучение персонала способам защиты засекреченной информации должно проводиться регулярно, потому что технология защиты требует постоянного обновления.

Обучение работника фирмы начинается с собеседования при приёме на работу и подписания им договора о неразглашении тайны и заканчивается его увольнением и подписанием договора, не допускающим использование секретных данных фирмы в каких-либо целях.

Основные положения по информационной безопасности при работе с персоналом.

• Ответственность за безопасность секретной информации входит в обязанности сотрудников, а именно за ресурсы, процессы и мероприятия по обеспечению защиты.

• Проводится проверка персонала при поступлении на работу, включая характеристики и рекомендации, резюме, образование и квалификацию, а также документы, удостоверяющие личность.

• Первостепенным условием при приёме на работу должно быть заключение договора о неразглашении служебной информации.

• Требования к персоналу, связанные с защитой конфиденциальной информации, и ответственность за её нарушение, должны быть внесены в трудовой договор.

Основные виды реализации угроз информационной безопасности:

1) завладение конфиденциальными данными, вследствие чего у злоумышленника оказывается их копия. Получение конфиденциальной информации может происходить при помощи разных методов: подслушивание разговоров сотрудников данного предприятия, использование технических средств (подслушивающих устройств), копирование секретных данных.

2) кража служебных документов, в результате чего злоумышленник овладевает секретными сведениями, а предприятие в свою очередь их лишается.

3) повреждение или полная ликвидация информации, в результате чего злоумышленник приносит вред предприятию.

4) изменение работником секретной информации, вследствие чего специалисты предприятия могут принять неверные руководящие действия.

Таким образом, самой часто встречающейся причиной осуществления угроз по защите безопасности является безответственность сотрудников предприятия. Это прослеживается в нарушении персоналом условий по защите информационной безопасности, что приводит к утечке секретной информации.

Утечка информации – это несанкционированный доступ к закрытым данным и неконтролируемое распространение секретных сведений в результате их разглашения.

Главные причины утечки информации:

• нарушение сотрудниками требований в работе с источниками служебной информации и правил использования систем защиты;

• недочёты в конструировании систем защиты;

• проведение злоумышленником технической и агентурной разведок.

Виды утечки информации:

• разглашение;

• несанкционированный доступ к информации;

• получение секретной информацией разведками.

Под разглашением информации понимается запрещённая передача служебной или секретной информации до людей, не имеющих на неё права.

Под несанкционированным доступом понимается получение запрещённой информации ложным или обманным путём лицом, не имеющим на неё права.

Получение секретной информации разведками может осуществляться с помощью технических средств или агентурными методами.

Канал утечки информации – это источник запрещённой информации – человек или материальный носитель.

Все каналы утечки конфиденциальной информации делятся на косвенные и прямые. Косвенные каналы не требуют прямого доступа к техническим средствам

информации. Прямые каналы – непосредственный доступ к источнику информации.

Примеры косвенных каналов утечки:

- похищение или потеря носителей информации;

- фотографирование, прослушивание на расстоянии;

- перехват электромагнитных излучений.

Примеры прямых каналов утечки:

- утечка информации из-за нарушения сотрудниками предприятия служебных требований;

- непосредственное копирование.

Способы защиты конфиденциальной информации на предприятии:

• Контроль сотрудников, обеспечивающих сохранность на территории предприятия всех носителей конфиденциальной информации, а также фото и видеоаппаратуры.

• Защита от неразрешённого доступа в помещения, в которых находятся компьютеры.

• При увольнении сотрудника, необходимо брать с него расписку о неразглашении секретной информации.

• Выбор ответственного лица, ведущего учет и контроль работников, занимающихся данными, содержащими конфиденциальную информацию, обеспечивающими хранение документов, их выдачу работникам под роспись и контроль возврата документации.

• Обеспечение специально организованных мест для приема посетителей.

Таким образом, при соблюдении всех правил безопасности персоналом предприятий можно избежать или свести к минимуму утечку секретной информации, которая может нанести колоссальный или необратимый вред организации.