Г.Н. Гудов, Г.Е. Шепитько

ПРОВЕДЕНИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время отмечается стремление криминальных и коммерческих структур, получить незаконным путем информацию, которой располагают различные организации. Для получения информации используются как современные технические средства, так и попытки непосредственного получения информации от лиц, располагающих ею. Поэтому благополучие и успешное финансовое и производственное развитие организаций напрямую зависят от обеспечения безопасности информации (конфиденциальность, целостность, доступность).

В связи с этим ставится задача оптимального распределения ограниченного материального ресурса с обязательным выполнением требований нормативных документов по защите информации.

На практике решение такой задачи наталкиваются на отсутствие исходных данных по зависимости финансовых затрат для обеспечения необходимого уровня защиты информации, количественных характеристик угроз и ущерба от реализации угроз, модели поведения правонарушителя и выбор оптимального варианта по эффективной защите информации.

Для решения данный задачи необходимо**:**

определить ***предмет защиты***;

установить ***источники угроз***, которые смогут воздействовать на предмет защиты;

классифицировать виды ***угроз***, которые при их реализации приведут к изменению качественных характеристик информационной безопасности (конфиденциальности, целостности, доступности);

разработать вероятностную ***модель поведения нарушителя*** (способы и методы реализации угроз);

провести ***анализ состояния защищенности информации*** в организации, выявить возможные каналы утечки, несанкционированного доступа к информации;

обосновать критерии выбора рационального варианта системы защиты информации (**СЗИ**);

разработать комплекс рекомендаций по обеспечению информационной безопасности.

Рассмотрим реализацию этих рекомендаций для физических носителей информации (бумажные, машинные носители информации и т.п.), находящихся в помещении.

К основными источниками угроз информационной безопасности можно отнести преступные группировки и отдельных лиц, работников организаций, стихийные природные явления (пожары, наводнения, ураганы, землетрясения и т.п.), отказы и сбои технических средств.

К основным угрозам безопасности физическим носителям информации можно отнести: разглашение информации, утрата (потеря, хищение, кража) носителей информации; несанкционированное копирование, чтение, наблюдение, фотографирование информации; нарушение целостности и достоверности информации, носителей информации; блокировка доступа законных пользователей к носителям информации.

При этом возможные следующие способы (методы) реализации угроз физическим носителям информации**:**

1. Несанкционированный проход на объект защиты с целью прослушивания, установок технических средств съема информации, сбора отходов производства, вывод из строя механизмов защиты объекта.

2. Несанкционированный доступ к физическим носителям информации, с целью хищения, чтения, копирования информации, уничтожения носителей информации.

3. Вербовка (подкуп, взятка и т.п.), психологическое и физическое воздействие на работника организации.

4. Нарушения работником требований нормативных документов по обеспечению режима секретности.

5. Случайные или ошибочные действия работника при эксплуатации технических средств защиты.

6. Преднамеренное изменение режима работы средств защиты информации.

7. Изменения режима работы средств защиты в результате воздействия стихийных бедствий, сбоя или отказа средств жизнеобеспечения.

На основании возможных способов и методов реализации угроз и анализа состояния защиты объекта составляется перечень необходимых организационных, технических мероприятий по защите объекта.

Для защиты физических носителей информации предлагается комплекс мероприятий:

Организационные:

1. Определение перечня сведений, подлежащих защите.

2. Сбор, обработка, анализ и прогнозирование возможных угроз информационной безопасности.

3. Разработка нормативно-правовых документов, определяющих порядок организации защиты сведений.

4. Регламентация работы лиц в вопросах обеспечения режима и информационной безопасности.

5. Обеспечение строгого режима доступа на объект защиты

6. Обеспечение строгого режима доступа к охраняемым сведениям.

7. Поддержание установленного режима работы с носителями информации, правил пользования средствами обработки и защиты информации.

8. Правильная организация ремонтно-профилактических работ и ремонта технических средств.

9. Правильная организация ремонтно-строительных работ на защищаемых объектах.

10. Создание эффективной системы обучения лиц, правилам обеспечения информационной безопасности.

11. Формирование у лиц, допущенных к охраняемым сведениям, чувства личной ответственности за сохранность информации.

12. Проведение служебной проверки по каждому случаю нарушений, попыток несанкционированного доступа к информации, а также при обнаружении других недостатков в защите информации

13. Контроль организации защиты информации.

14. Контроль выполнения лицами требований и норм по защите информации.

Технические:

1. Инженерно-технические средства, обеспечивающие предотвращение несанкционированного доступа посторонних лиц на объекты защиты.

2. Технический контроль эффективности средств защиты информации.

Предложенный комплекс мероприятий использовался в подразделениях ФСНП России.