

Практическая работа

Тема: Определение объектов защиты на типовом объекте информатизации

Цель: научиться определять объекты защиты на типовом объекте информатизации

Теоретические сведения

Защита информации должна быть системной, включающей в себя различные взаимосвязанные компоненты. Важнейшим из этих компонентов являются объекты защиты, ибо от их состава зависят и методы, и средства защиты и состав мероприятий.

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

В соответствии с данным определением можно классифицировать объекты защиты в соответствии с рисунком 1

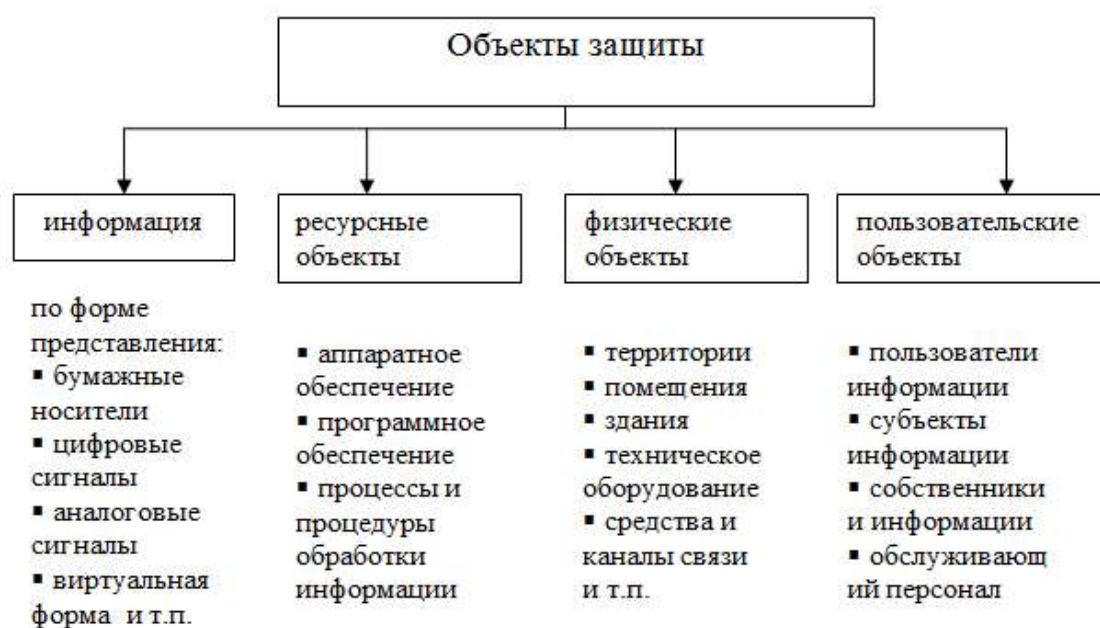


Рис. 1. Классификация объектов защиты

В качестве объекта защиты часто рассматривается *объект* информатизации. *Объект* информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. ФСТЭК в своих руководящих документах трактует данное понятие несколько иначе.

Под объектами информатизации, аттестуемыми *по* требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

В отношении любого объекта информатизации справедливы следующие утверждения:

1. Объект информатизации создан ради осуществления какой-то деятельности - основной деятельности.

2. Информационные технологии на объекте информатизации служат для реализации целей основной деятельности.
3. Состояние объекта информатизации динамически меняется под влиянием внешних и внутренних факторов.

Защищаемыми объектами информатизации в соответствии с СТР-К (Специальные требования и рекомендации по технической защите конфиденциальной информации, утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282) являются:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации (Основные технические средства и системы - ОТСС);
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается/циркулирует (вспомогательные технические средства - ВТСС);
- защищаемые помещения.

Практическое задание

1. В соответствии с вариантом определите для вашей организации 5 наиболее важных объектов защиты, свой выбор обоснуйте.
2. Для каждого объекта защиты определите ценность (от 1 до 5), обоснуйте ваш выбор.
3. Для каждого объекта защиты подберите по 1 возможной уязвимости.
4. Для каждой уязвимости подберите по возможной угрозе.
5. Проанализировав все уязвимости и угрозы дайте оценку риска каждой угрозы (низкий, средний, высокий). Ответ обоснуйте.

Варианты

- | | |
|---|-----------------------------------|
| 1. Отделение коммерческого банка | 16. Офис благотворительного фонда |
| 2. Поликлиника | 17. Издательство |
| 3. Колледж | 18. Консалтинговая фирма |
| 4. Офис страховой компании | 19. Рекламное агентство |
| 5. Рекрутинговое агентство | 20. Отделение налоговой службы |
| 6. Интернет-магазин | 21. Офис нотариуса |
| 7. Центр оказания государственных услуг | 22. Бюро перевода (документов) |
| 8. Отделение полиции | 23. Научно проектное предприятие |
| 9. Аудиторская компания | 24. Брачное агентство |
| 10. Дизайнерская фирма | 25. Редакция газеты |
| 11. Офис Интернет-провайдера | 26. Гостиница |
| 12. Офис адвоката | 27. Праздничное агентство |
| 13. Компания по разработке ПО для сторонних организаций | 28. Городской архив |
| 14. Агентство недвижимости | 29. Диспетчерская служба такси |
| 15. Туристическое агентство | 30. Железнодорожная касса |

Контрольные вопросы

1. Что такое уязвимость и угроза ИБ?
2. Что такое риск информационной безопасности, для чего оценивать риски?
3. Что такое объект защиты информации? Приведите примеры.
4. Что такое объект информатизации, приведите примеры?
5. Что такое источник угрозы, приведите примеры.