Тип работы: Лабораторная работа

Предмет: Информатика

-

Виды угрозы информации могут быть классифицированы по ориентации на ресурсы и по природе возникновения. Рассмотрим каждый вид более подробно:
по ориентации на ресурсы:
oУгрозы конфиденциальности. Направлены на несанкционированный доступ к конфиденциальной информации и ее раскрытие третьим лицам. Это может включать кражу данных, несанкционированный доступ к системам или прослушивание коммуникаций.
oУгрозы целостности. Направлены на намеренное или случайное повреждение или изменение информации, что может привести к потере ее достоверности или целостности. Примеры включают вирусы, злонамеренное программное обеспечение или несанкционированное изменение данных.
oУгрозы доступности. Направлены на препятствование или нарушение доступности информации или ресурсов. Это может быть вызвано атаками на сеть, отказом сервисов, физическими разрушениями или прочими факторами, мешающими нормальной работе систем.
По природе возникновения:
oАбсолютные угрозы. Возникают из-за естественных явлений или непреднамеренных действий без вмешательства злоумышленников. Например, это может быть физическое повреждение оборудования в результате пожара, наводнения или стихийного бедствия.
oЧеловеческие угрозы. Связаны с намеренными действиями или ошибками, допущенными людьми. Включает в себя акты мошенничества, хищение данных, неправомерное использование доступа, физическую кражу или потерю устройств с данными.
oТехнические угрозы. Возникают из-за проблем или уязвимостей в технических системах и программном обеспечении. Это может включать вредоносные программы, отказы оборудования
oСоциальные угрозы. Связаны с межличностными взаимодействиями и социальными инженерными методами, направленными на манипуляцию и обман людей для получения несанкционированного доступа к информации. Примерами могут быть фишинг, поддельные запросы на информацию или обман сотрудников для раскрытия конфиденциальных данных.
oЕстественные угрозы. Связаны с естественными явлениями, такими как пожары, наводнения, землетрясения и т.д., которые могут привести к потере информации и нарушению доступности ресурсов.

Важно отметить, что угрозы информации могут пересекаться и взаимодействовать друг с другом. Например, злонамеренное программное обеспечение (техническая угроза) может привести к утечке конфиденциальной информации (угроза конфиденциальности) и нарушению доступности ресурсов (угроза доступности).
Для эффективной защиты информации необходимо учитывать все виды угроз и принимать соответствующие меры по предотвращению, обнаружению и реагированию на них. Это включает использование средств защиты информации, регулярное обновление и аудит систем, обучение пользователей и строгое соблюдение политик безопасности информации.

Задание 2. Изучить понятия и провести сравнительный анализ
Конфиденциальность компонента системы означает, что информация, содержащаяся в данном компоненте, доступна исключительно авторизованным пользователям или системам. Это означает, что только те лица или сущности, которым предоставлены соответствующие права доступа, имеют возможность просматривать, использовать или раскрывать информацию, хранящуюся в компоненте. Конфиденциальность обеспечивает защиту от несанкционированного доступа и утечки конфиденциальных данных.

Целостность компонента системы означает, что компонент находится в ожидаемом и неизменном

состоянии, и его данные не подверглись несанкционированным изменениям или повреждениям. Целостность гарантирует, что информация в компоненте остается точной, неповрежденной и нескомпрометированной. Любые попытки изменения данных в компоненте будут обнаружены и предотвращены, чтобы сохранить целостность системы и ее компонентов.

-