МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНСТИТУТ СФЕРЫ ОБСЛУЖИВАНИЯ И ПРЕДПРИНИМАТЕЛЬСТВА (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» В Г. ШАХТЫ РОСТОВСКОЙ ОБЛАСТИ
(ИСОиП (филиал) ДГТУ в г. Шахты)

Кафедра *КЭС*

Презентация

На тему: Методы защиты информации на предпртятии

по дисциплине Организация работы оператора электронно-вычисли тельных и вычислительных машин

Специальность

09.02.03 Программирование в компьютерных системах

Выполнил
обучающийся группы КВ9-220Б _____ Иваненко К.В
подпись расшифровка подписи

Проверил _____ преподаватель И.Ю. Бабенко
подпись

2021 г.

Содержание

Введение

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность не только становится обязательной, она еще и одна из характеристик ИС.

Под *безопасностью ИС* понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на ИС.

Виды умышленных угроз информации

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов ИС, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

1. утечка конфиденциальной информации;

2. компрометация информации;

3. несанкционированное использование информационных ресурсов;

4. ошибочное использование информационных ресурсов;

5. несанкционированный обмен информацией между абонентами;

6. отказ от информации;

7. нарушение информационного обслуживания;

8. незаконное использование привилегий.

Несанкционированный доступ

Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

1. перехват электронных излучений;

2. применение подслушивающих устройств (закладок);

3. дистанционное фотографирование;

4. перехват акустических излучений и восстановление текста принтера;

5. копирование носителей информации с преодолением мер защиты;

6. маскировка под зарегистрированного пользователя;

7. маскировка под запросы системы;

8. использование программных ловушек;

9. незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;

10. злоумышленный вывод из строя механизмов защиты;

11. расшифровка специальными программами зашифрованной: информации;

Методы и средства защиты информации

Методы защиты информации:

1. Управление доступом. Управление представляет собой направленное воздействие на ресурсы системы в рамках установленного технологического цикла обработки и передачи данных, где в качестве ресурсов рассматриваются технические средства, ОС, программы, элементы данных и т.п.

2. Препятствие - физически преграждают нарушителю путь к защищаемым данным.

3. Маскировка представляет собой метод защиты данных путем их криптографического закрытия.

4. Побуждение состоит в создании такой обстановки и условий, при которых правила обращения с защищенными данными регулируются моральными и нравственными нормами.

5. Принуждение включает угрозу материальной, административной и уголовной ответственности за нарушение правил обращения с защищенными данными.

На основе перечисленных методов создаются средства защиты данных. Все средства защиты данных можно разделить на формальные и неформальные:

1.Формальные средства защиты.

Формальными называются такие средства защиты, которые выполняют свои функции по заранее установленным процедурам без вмешательства человека. К формальным средствам защиты относятся технические и программные средства.
1) К техническим средствам (вам защиты относятся все устройства, которые предназначены для защиты. Физическими называются средства защиты, которые создают физические препятствия на пути к защищаемым данным и не входят в состав аппаратуры ИВС, а аппаратными - средства защиты данных, непосредственно входящие в состав аппаратуры ИВС.
2) Программными называются средства защиты данных, функционирующие в составе программного обеспечения ИВС.

2.Неформальные средства защиты.

Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей, либо регламентируют эту деятельность. Неформальные средства включают организационные, законодательные и морально-этические меры и средства.
1)Под организационными средствами защиты понимаются организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации ИВС для обеспечения безопасности данных.
2)К морально-этическим нормам защиты относятся всевозможные нормы, которые традиционно сложились или складываются по мере развития информатизации общества. Такие нормы не являются обязательными, однако их несоблюдение ведет, как правило, к потере авторитета, престижа человека, группы лиц или целой организации. Считается, что Этические нормы оказывают положительное воздействие на персонал и пользователей. Морально-этические нормы могут быть неписаными (например, общепринятые нормы честности, патриотизма и т.п.) и оформленными в качестве свода правил и предписаний (кодексов).

Заключение

Исследования подтверждают, что во всех странах убытки от злонамеренных действий непрерывно возрастают. Причем основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними, т.е. с нереализованностью системного подхода. Поэтому необходимо опережающими темпами совершенствовать комплексные средства защиты.

Потребность в защите информации зависит от рода выполняемой вами работы и от чувствительности информации, которой вы управляете. Однако все хотят секретности и чувства безопасности, которое появляется вместе с обоснованной уверенностью в том, что они не могут стать жертвой нарушения защиты информации.

Список используемых источников

1.https://ru.wikipedia.org