Безопасность в информационных системах экономики

Информационные технологии в экономике
Лекция 7 (15)

К.т.н., доц., Васина Е.Н.

- Понятие информационной безопасности
- Основные определения и критерии классификации угроз
- Классификация вредительских программ
- Принципы обеспечения ИБ
- Правовые основы обеспечения безопасности
- Методы и средства защиты информации

Факторы, определяющие важность ИБ

- национальные интересы, угрозы им и обеспечение защиты от этих угроз выражаются, реализуются и осуществляются через *информацию* и *информационную* сферу;
- человек и его права, *информация и информационные системы* и права на них - основные объекты информационной безопасности;
- решение задач национальной безопасности связано с использованием *информационного подхода* как основного научно-практического метода;
- проблема национальной безопасности имеет ярко выраженный *информационный характер*.

- ***Информационная безопасность*** - защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*.
- ***Защита информации*** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

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.

Основные аспекты ИБ

- **Доступность** – это возможность за приемлемое время получить требуемую информационную услугу.
- **Целостность -** актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
- **Конфиденциальность** – это защита от несанкционированного доступа к информации.

- ***Угроза*** - потенциальная возможность определенным образом нарушить информационную безопасность.
- ***Атака - п***опытка реализации *угрозы* называется а ***Злоумышленник*** предпринимает такую попытку.
- Потенциальные *злоумышленники* - ***источники угрозы***.
- *Угроза* - следствие наличия *уязвимых* мест в защите информационных систем.
- Промежуток времени от появления слабого места до его ликвидации называется ***окном опасности***, ассоциированным с данным *уязвимым* местом.

Критерии классификации угроз:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого *угрозы* направлены в первую очередь;
- по компонентам информационных систем, на которые *угрозы* нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению *источника угроз* (внутри/вне рассматриваемой ИС).

Угрозы доступности

- *непреднамеренные ошибки* пользователей ИС
- *отказ пользователей*;
- *внутренний отказ* информационной системы;
- *отказ поддерживающей инфраструктуры.*

Угрозы целостности

Нарушение статической целостности
(неизменность информационных объектов):

- ввести неверные данные;
- изменить данные.

Угрозы динамической целостности
(корректное выполнение сложных операций – транзакций) :

- нарушение атомарности транзакций,
- переупорядочение,
- *кража*,
- дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.).

Угрозы конфиденциальности

- перехват данных
- методы морально-психологического воздействия
- злоупотребление полномочиями

Случайные угрозы

- *Стихийные бедствия и аварии*
- *Сбои и отказы*
- *Ошибки при разработке ИС, алгоритмические и программные* ошибки
- Ошибки пользователей и обслуживающего персонала

Преднамеренные угрозы

- *традиционный шпионаж и диверсии*
- *несанкционированный доступ к информации*
- *электромагнитные излучения и наводки*
- *несанкционированная модификация технической структуры*
- *несанкционированное изменение программной структуры*

Вредоносное программное обеспечение

Характеристики вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Вредоносная функция :

- внедрение другого вредоносного ПО;
- получение контроля над атакуемой системой;
- агрессивное потребление ресурсов;
- изменения или разрушения программ и/или данных.

Способ распространения:

- ***вирусы*** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы (для активизации *вируса* требуется запуск зараженной программы);
- ***"черви"*** - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение.

Классификация вредоносных программ (по Касперскому)

1. Программы, непосредственно выполняющие деструктивную функцию (собственно вредительские программы):
   - вирусы;
   - черви;
   - троянские программы.
2. Программы, обеспечивающие выполнение программ с деструктивной функцией:
   - подозрительные упаковщики;
   - вредоносные утилиты;
   - условно нежелательные программы (Adware и Riskware).

По назначению вредительские программы

- шпионские программы (Spyware);
- программы рассылки спама (Adware);
- программы перехвата сообщений в сети;
- программы скрытого удаленного администрирования (Rootkit, Backdoor).

"Программный *вирус* - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах « (ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения«)

Признаки заражения компьютера вирусами

- программы перестают запускаться или внезапно останавливаются в процессе работы,
- увеличивается длина исполняемых файлов,
- быстро сокращается объем свободной дисковой памяти,
- замедляется работа некоторых программ,
- в текстовых файлах появляются бессмысленные фрагменты,
- па экране появляются странные сообщения, которые раньше не наблюдались,
- появляются файлы со странными датами и временем создания,
- операционная система перестает загружаться,
- данные на носителях портятся.

Заражаемые объекты:

- **Исполняемые файлы**.
- **Загрузчик операционной системы и главная загрузочная запись жесткого диска.**
- **Файлы документов, информационные файлы баз данных, таблицы табличных процессоров** и другие аналогичные файлы могут быть заражены **макровирусами.**

Принципы обеспечения ИБ

1. Обеспечение ИБ выполняется в соответствии с политикой управления информационными рисками (ИР), разработка и реализация которой осуществляется под непосредственным руководством первых лиц предприятия с привлечением менеджмента соответствующих служб и отделов.
2. Оптимальный баланс затрат на управление ИР и общего ущерба от ИР.
3. Система управления ИР является централизованной и реализует единую политику управления.
4. ИБ достигается за счет комплексного использования нормативных, экономических и организационных мер, технических, программных и криптографических средств.
5. Система управления должна быть многоуровневой и равнозащищенной во всех звеньях.

Принципы обеспечения ИБ

6. Д. б. обеспечена непрерывность функционирования на всех жизненных циклах системы.
7. Д. б. обеспечено разграничение и ограничение доступа персонала к информации.
8. Система д. б. способна к развитию и адаптации к изменению условий функционирования.
9. Наличие системы непрерывного мониторинга за выполнением *всем* персоналом установленных правил работы в ИС.
10. Мониторинг и аудит эффективности ИС и своевременная ее модернизация.

Правовые основы обеспечения безопасности

- законодательная база
- система национальных стандартов в информационной сфере

Организационные методы управления информационными рисками

- методы применения средств управления;
- методы непосредственного управления информационными рисками;
- методы общего менеджмента.

Защита от случайных угроз

- *Дублирование* информации или резервное копирование
- *Повышение надежности и отказоустойчивости* ИС
- *противодействия техногенным авариям и стихийным бедствиям*
- *сокращение ошибок пользователей и обслуживающего персонала*

Защита от преднамеренных угроз

- Система охраны объекта ИС (инженерные конструкции; охранная сигнализация; средства наблюдения; подсистема доступа на объект; дежурная смена охраны).
- Организация работ с конфиденциальными информационными ресурсами на объектах ИС
- Противодействие наблюдению в оптическом диапазоне
- Противодействие подслушиванию
- Защита от злоумышленных действий обслуживающего персонала и пользователей
- Защита от несанкционированного доступа к информации (система разграничения доступа к информации)