Информационная безопасность

Лектор :к. т.н., доцент
Квятковский Юрий Григорьевич
Каф. «Прикладная информатика»

Литература:

а) основная:

- *Мельников В.П.* Информационная безопасность и защита информации: учебное пособие для вузов/Мельников В.П. В.П. Мельников, С.А.Клейменов,А.М.Петраков,-М.: Академия,2007.-336с.;
- *Одинцов А.А.* Экономическая и информационная безопасность предпринимательства: учебное пособие для вузов/Одинцов А.А. ,-М.:Академия,2006.-336с.

б) дополнительная:

- *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие для вузов/Малюк А.А. ,-М.:Горячая линия-Телеком,2004.-280с.

Литература:

в) периодические издания:

- Журнал «Мир ПК»;
- Журнал «Стандарты и качество»;
- Журнал «Техническая кибернетика».

г) интернет-ресурсы:

- www.infosecurity.ru – Проект InfoSecurity.ru - информационная безопасность бизнеса;
- all-ib.ru – Информационная безопасность, защита информации;
- z-oleg.com – Конференции по информационной безопасности.

Информационная безопасность

Предмет защиты

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

Особенности информации:

- она нематериальна;
- информация хранится и передается с помощью материальных носителей;
- любой материальный объект содержит информацию о самом себе или о другом объекте.

Свойства информации

1. Информация доступна человеку, если она содержится на материальном носителе.
2. Информация имеет ценность.
3. Ценность информации изменяется во времени.
4. Информация покупается и продается.
5. Сложность объективной оценки количества информации.

Информационная безопасность

2. Информация имеет ценность

Умышленно искаженная информация называется ***дезинформацией.***
Информация доступ к которой ограничен называется ***конфиденциальной.***
Виды конфиденциальной информации:

- содержащая государственную тайну,
- содержащая коммерческую тайну.

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п.
Государственную тайну могут содержать сведения, принадлежащие государству (государственному учреждению).
Три возможные степени (грифы) секретности сведений, содержащих государственную тайну:

«секретно»,
«совершенно секретно»,
«особой важности».

Три категории ценности конфиденциальной коммерческой информации:

«коммерческая тайна - строго конфиденциально»;
«коммерческая тайна - конфиденциально»;
«коммерческая тайна».

Информационная безопасность

3. Ценность информации

По А.А. Харкевичу- предлагается принять за меру ценности информации количество информации, необходимое для достижения поставленной цели, т. е. рассчитывать приращение вероятности достижения цели. Так, если до получения информации вероятность достижения цели равнялась P_0, а после ее получения - P_1, то ценность информации определяется как логарифм отношения P_1/P_0. Ценность информации при этом измеряется в битах.

$$I = \log \frac{P_1}{P_0}$$

Ценность может быть как положительной так и отрицательной. Такая информация называется ***дезинформацией.*** Ценность информации меняется во времени.

Информационная безопасность

4. Информация покупается и продается

Пути получения информации:

- проведение научных исследований;
- покупка информации;
- противоправное добывание информации.

Использование информации:

- продается на рынке;
- внедряется в производство для получения новых технологий и товаров, приносящих прибыль;
- используется в научных исследованиях;
- позволяет принимать оптимальные решения в управлении.

5. Сложность объективной оценки количества информации

Подходы к измерению количества информации

- *Энтропийный подход.*
- *Тезаурусный подход.*
- *Практический подход.*

Энтропийный подход

$$I = Ni = \sum_{i=1}^{k} P_i \log_2 P_i$$

Pi - вероятность появления в сообщении символа i;

к - количество символов в алфавите языка.

Тезаурусный подход

Структурированные знания, представленные в виде понятий и отношений между ними, называются ***тезаурусом.***

Увеличение тезауруса осуществляется за счет:

- обучения,
- покупки лицензии,
- приглашения квалифицированных сотрудников,
- хищения информации.

Тенденции изменения тезаурусов:

- развитие тезаурусов отдельных элементов,
- выравнивание тезаурусов элементов общества.

Информационная безопасность

Практический подход

На практике количество информации измеряют, используя понятие ***«объем информации».*** Количество информации может измеряться в количестве бит (байт), в количестве страниц текста и т.п.

Предмет защиты - информация, хранящаяся, обрабатываемая и передаваемая в информационных системах (ИС).

Особенностями этой информации являются:

- двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрация большого количества информации в ИС.

Информационная безопасность

***Безопасность (защищенность) информации* в ИС -** это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.

Информационные системы, в которых обеспечивается безопасность информации, называются ***защищенными.***

Информационная безопасность достигается проведением руководством соответствующего уровня ***политики информационной безопасности.***

Основным документом, на основе которого проводится политика информационной безопасности, является ***программа информационной безопасности.***

Информационная безопасность

Понятие информационной безопасности

Под ***информационной безопасностью*** понимается 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.

Информационная безопасность

Основные составляющие информационной безопасности

Категории информационной безопасности – обеспечение: ***доступности, целостности*** и ***конфиденциальности*** информационных ресурсов и поддерживающей инфраструктуры

- **Составляющие ИБ**
  - **конфиденциальность**
  - **целостность**
  - **доступность**

Информационная безопасность

Основные составляющие информационной безопасности

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

Целостность подразделяется на ***статическую*** (понимаемую как неизменность информационных объектов) и ***динамическую*** (относящуюся к корректному выполнению сложных действий (транзакций).

Информационная безопасность

Возможные ***экономические последствия атак*** на информацию

1. Раскрытие коммерческой информации может привести к серьезным ***прямым убыткам*** на рынке.

2. Известие о краже большого объема информации обычно серьезно влияет на ***репутацию фирмы***, приводя косвенно к потерям в объемах торговых операций.

3. Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки.

4. Подмена информации как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам.

5. Многократные успешные атаки на фирму, предоставляющую какой-либо вид информационных услуг, ***снижают доверие*** к фирме у клиентов, что сказывается на объеме доходов.

Информационная безопасность

Категории информации с точки зрения информационной безопасности:

- ***конфиденциальность*** - гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется ***хищением*** информации,
- ***целостность*** - гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется ***фальсификацией сообщения,***
- ***аутентичность*** - гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется ***фальсификацией автора сообщения,***
- ***апеллируемость*** - гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек.

Информационная безопасность

Категории информационных систем с точки зрения информационной безопасности:

- ***надежность*** - гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано,
- ***точность*** - гарантия точного и полного выполнения всех команд,
- ***контроль доступа*** - гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются,
- ***контролируемость*** - гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса,
- ***контроль идентификации*** - гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает,
- ***устойчивость к умышленным сбоям*** - гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.