ТЕМА 1. Информационная безопасность компьютерных систем. Информационные сети. Основы безопасности. Общие определения.

1.1. Основные понятия и терминология.

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах.

Информационный объект — среда, в которой информация создается, передается, обрабатывается или хранится.

Безопасность информационного объекта — его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

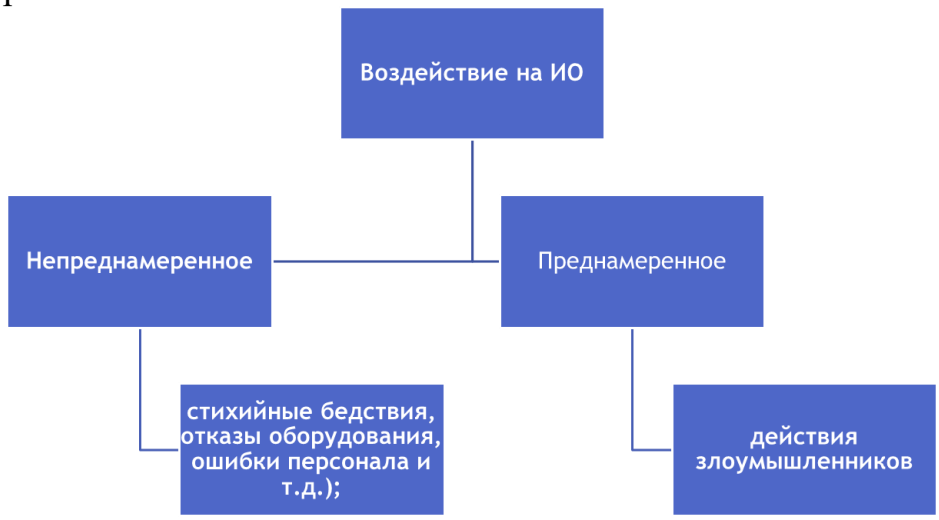

Рисунок 1. Воздействие на информационный объект

В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ.

Несанкционированный доступ — получение нарушителем доступа к объекту в нарушение установленных правил.

Угроза информационной безопасности объекта — возможные воздействия на ИО, приводящие к ущербу.

Уязвимость — некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы.

Атака — действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости.

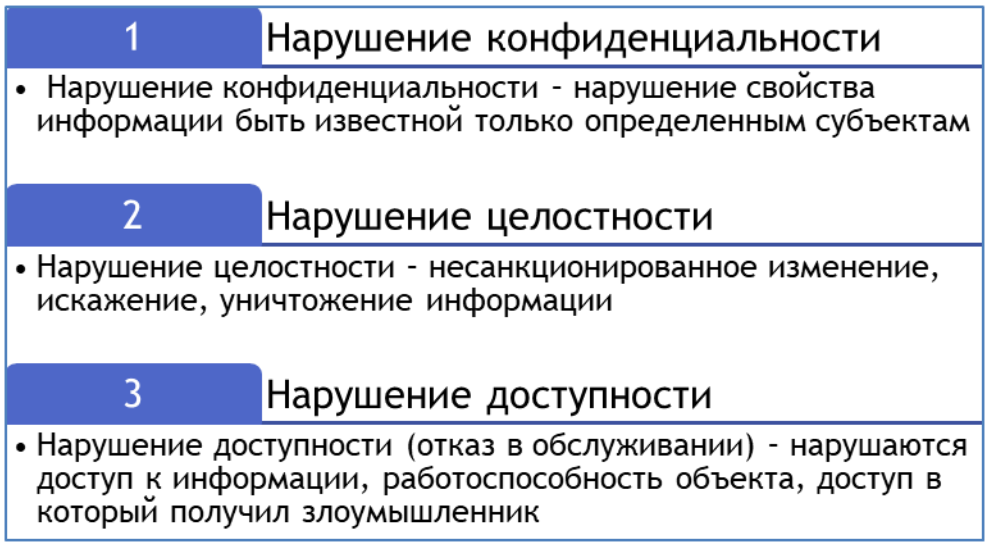

Рисунок 2. Несанкционированный доступ

Комплексная защита информационного объекта.

Цель защиты информационного объекта — противодействие угрозам безопасности.

Защищенный информационный объект — это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплексная защита информационного объекта (ИО) — совокупность методов и средств (правовых, организационных, физических, технических, программных).

Политика безопасности — совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от заданного множества угроз безопасности.

1.2 Классификация угроз информационной безопасности.

Случайные угрозы

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала.

Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).

Преднамеренные угрозы

Преднамеренные угрозы связаны с действиями людей (работники спецслужб, самого объекта, хакеры).

Огромное количество разнообразных информационных объектов делает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов.

Рисунок 3. Классификация угроз информационной безопасности

Несанкционированный доступ к информации вычислительной системы может быть осуществлен через:

- Штатные каналы доступа, если нет никаких мер защиты (терминалы пользователей, терминал администратора системы, удаленные терминалы);
- Нештатные каналы доступа (побочное электромагнитное излучение информации с аппаратуры системы, побочные наводки информации по сети электропитания и заземления, побочные наводки информации на вспомогательных коммуникациях, подключение к внешним каналам связи).

1.3. Классификация методов защиты информации

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

Законодательные (правовые).

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

Организационные.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации.

К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Технические.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства.

В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Критерий "эффективность-стоимость"

Принципиальным вопросом при определении уровня защищенности объекта является выбор критериев. Рассмотрим один из них - широко известный критерий "эффективность - стоимость".

Пусть имеется информационный объект, который при нормальном (идеальном) функционировании создает положительный эффект (экономический, политический, технический и т.д.).

Этот эффект обозначим через E_0.

Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.).

Обозначим величину ущерба - *DE*.

Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

$$E = E_0 - \Delta E. \qquad 1)$$

Относительная эффективность:

$$\delta = \frac{E}{E_0} = \frac{E_0 - \Delta E}{E_0} = 1 - \frac{\Delta E}{E_0}. \qquad 2)$$

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от DE:

$$U = f(\Delta E). \qquad 3)$$

Будем считать, что установка на объект средств защиты информации уменьшает негативное действие несанкционированного доступа на эффективность функционирования объекта. Обозначим снижение эффективности функционирования объекта при наличии средств защиты через $DE_{З,}$ а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект - через К, тогда:

$$\Delta E_З = \frac{\Delta E}{K}, \qquad 4)$$

где К³1.
Выражения (1) – (2) примут вид:

$$E_З = E_0 - \Delta E_З = E_0 - \frac{\Delta E}{K}, \qquad 5)$$

$$\delta_З = \frac{E_З}{E_0} = \frac{E_0 - \Delta E_З}{E_0} = 1 - \frac{\Delta E_З}{E_0} = 1 - \frac{\Delta E}{K E_0}. \qquad 6)$$

Стоимость средств защиты зависит от их эффективности, и в общем случае К — есть возрастающая функция от стоимости средств защиты:

$$K = f(C). \qquad 7)$$

Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту:

$$U_\Sigma = \frac{U}{K} + C = \frac{U}{f(C)} + C. \qquad 8)$$

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то U_S непосредственно изменяет эффективность:

$$E_З = E_0 - \frac{\Delta E}{K - C} \qquad 9)$$

Таким образом, классическая постановка задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

$$\begin{matrix} U_\Sigma \to \min \\ C = C_{опт} \end{matrix}, \qquad 10)$$

или

$$\begin{matrix} E_Ç \to \max, & \delta_Ç \to \max, \\ C = C_{îïò} & C = C_{îïò}. \end{matrix} \qquad 11)$$

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется отсутствием зависимостей K = f(C) и особенно ущерба от несанкционированного доступа. И если зависимость коэффициента защищенности от стоимости средств защиты можно получить, имея технические и стоимостные характеристики доступных средств защиты, то оценить реальный ущерб от несанкционированного доступа чрезвычайно трудно, так как этот ущерб зависит от множества трудно прогнозируемых

факторов: наличия физических каналов несанкционированного доступа, квалификации злоумышленников, их интереса к объекту, последствий несанкционированного доступа и т.д.

Вместе с тем для объектов, на которые возлагаются ответственные задачи и для которых несанкционированный доступ влечет катастрофические потери эффективности их функционирования, влиянием стоимости средств защиты на эффективность можно пренебречь, т.е. если:

$$C << U, \tag{12}$$

то:

$$U_{\Sigma} = \frac{U}{f(C)}. \tag{13}$$

В этом случае (11) и (12) принимают вид:

$$\begin{aligned} U_{\Sigma} &\to \min, \\ C &\le C_{доп} \end{aligned} \tag{14}$$

Или:

$$\begin{aligned} E_З \to \max, \quad & \delta_З \to \max, \\ C \le C_{доп}, \quad & C \le C_{доп}, \end{aligned} \tag{15}$$

где $C_{доп}$ — допустимые расходы на защиту.