# Защита информации в автоматизированных системах

## Политика безопасности

**Политика безопасности** – набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе.

Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации

**Субъект** – активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы.

**Объект** – пассивный компонент системы, хранящий, принимающий или передающий информацию.

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы.

В два вида политики безопасности

– избирательная

– полномочная

***Избирательная политика безопасности***

Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

– все субъекты и объекты системы должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего правила

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа. Модель называется матричной.

объект системы (О*1*…О*n*)

субъект (С*1*…С*n*)

(Read Only), «доступ на запись»

(Write Only), «доступ на чтение-запись»

(Read-Write) и др.

|  |
| --- |
|  |

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе

***Полномочная политика безопасности***

Полномочная политика безопасности подразумевает:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападула. В упрощенном виде они определяют, что информация может передаваться только «наверх». **Пример** если имеется доступ к секретам гос важности, то будет доступен и доступ ниже, но не выше.

Основное назначение полномочной политики безопасности

– регулирование доступа субъектов системы к объектам с различным уровнем критичности

– предотвращение утечки информации с верхних уровней на нижние

– блокирование возможных проникновений с нижних уровней на верхние.

***Управление информационными потоками***

**Каналы объекта** – взаимодействии субъекта и объекта возникает некоторый поток информации от субъекта к объекту.

Избирательное и полномочное управление доступом, а также управление информационными потоками – то, на чем строится вся защита.

## Механизмы защиты

**Достоверная вычислительная база** (ДВБ) – абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.

Основой ДВБ является **ядро безопасности** – элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам.

Монитор ссылок – абстрактной концепции механизма защиты.

Помимо ядра безопасности ДВБ содержит другие механизмы, отвечающие за жизнедеятельность системы. К ним относятся планировщики процессов, диспетчеры памяти, программы обработки прерываний, примитивы ввода – вывода и тд.

Под базой данных защиты понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам.

**Профиль** – список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым субъектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа.

**Мандат или билет.** Это элемент МД, определяющий тип доступа определенного субъекта к определенному объекту

**Идентификация, аутентификация и авторизация субъектов и объектов системы.** Эти функции необходимы для подтверждения подлинности субъекта, законности его прав на данный объект или на определенные действия,

**Регистрация и протоколирование. Аудит.** Эти функции обеспечивают получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля

**Противодействие «сборке мусора».** После окончания работы программы обрабатываемая информация не всегда полностью удаляется из памяти.

**Контроль доступа.** Под контролем доступа будем понимать ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности. Под

## Принципы реализации политики безопасности

Общие принципы

**Группирование.**

**Правила умолчания**

**Минимум привилегий.** Каждый пользователь и процесс должен иметь минимальное число привилегий, необходимых для работы.

**«Надо знать».** Доступ разрешен только к той информации, которая необходима пользователям для работы.

**Объединение критичной информации.** Во многих системах сбор, хранение и обработка информации одного уровня производится в одном месте (узле сети, устройстве, каталоге).

**Привилегии владельца.** Владелец обладает всеми разрешенными для этого типа данных правами на объект

**Свободная передача привилегий.** При такой схеме субъект, создавший объект, может передать любые права на него любому другому субъекту

Интеллектуальная деятельность

Интеллектуальная собственность(ИС)

Объект ИС – **охраноспособный** результат интеллектуальной деятельности, создаются интеллектуальные права создателя.

Первый патентный закон 1623г.

**Классификация ОИС:**

* право промышленной собственности – область техники
* авторское(смежное) право – область культуры и искусства

Объекты авторского права характеризуются: произведения науки, литературы и искусства, компьютерные программы (программы для ЭВМ);

Объекты смежных прав характеризуются: исполнения, фонограммы, передачи организации кабельного вещания, включая интернет.

Объекты права промышленной собственности характеризуются: изобретения, полезные модели и промышленные образцы

**Патент выдается на:**

Изобретения – самый важный объект ис, который может состоять из вещества и предмета

Полезная модель – промышленный образец и селекционные достижения

Топологии интегральных микросхем

Секреты производства

Фирменные наименования

Товарные знаки и знаки обслуживания

Географические указания:

а) указание места происхождения товара

б) наименование места происхождения товара

Экономическая роль ИС

Роль ИС – экономическая.

Авторское право и смежные права

Основная цель охраны авторских прав – это содействие обогащению и распространению национального культурного наследия.

Авторское право возникает в силу факта их создания.

**Объектами охраны** могут быть как хорошие произведения, так и плохие.

Заложенные в эти произведения идеи не обязательно должны быть новыми. Форма содержания должна быть оригинальной

* Литературные произведения.
* Научные произведения
* Драматические произведения
* Хореографические произведения
* Аудио-видео произведения
* Произведения архитектуры
* Компьютерные программы, базы данных

Объектами авторского права **не являются:**

* Официальные документы
* Государственные символы
* Произведения народного творчества, авторы которого не известны.

**Субъекты авторского права** – лица, которым по закону, как создателям произведения, принадлежит авторское право. Автором произведения считается лицо, указанное в качестве автора в оригинале произведения, пока не доказано обратное

**Авторский договор** необходим для разделения прав собственности на объект.

Неимущественные права

* Право авторства
* Право на имя
* Право на защиту репутации
* Право на обнародование произведения.

Имущественные права:

* Воспроизведение произведения
* Распространение оригинала
* Прокат оригинала
* Публичный показ
* Передачу в эфир
* Перевод произведения на другой язык, или изменение

Охрана смежных прав – права исполнителей на исполняемые произведения

* Права тех, кто оказывает помощь авторам в доведении произведения до публики

Для возникновения прав не требуется выполнение формальностей.

Промышленная собственность.

Патенты и объекты патентования

Патент – это выдаваемый патентным органом от имени гос-ва документ, который удостоверяет:

1 Авторство

2 Приоритет

3 Исключительное право на его использование