Лекция №1

Методы защиты операционных систем от существующих угроз

Задачи операционных систем в рамках информационной безопасности

- Обеспечение конфиденциальности обрабатываемых данных.
- Обеспечение целостности обрабатываемых данных.
- Подотчётность ресурсов системы.

Информационные процессы, защищаемые средствами ОС

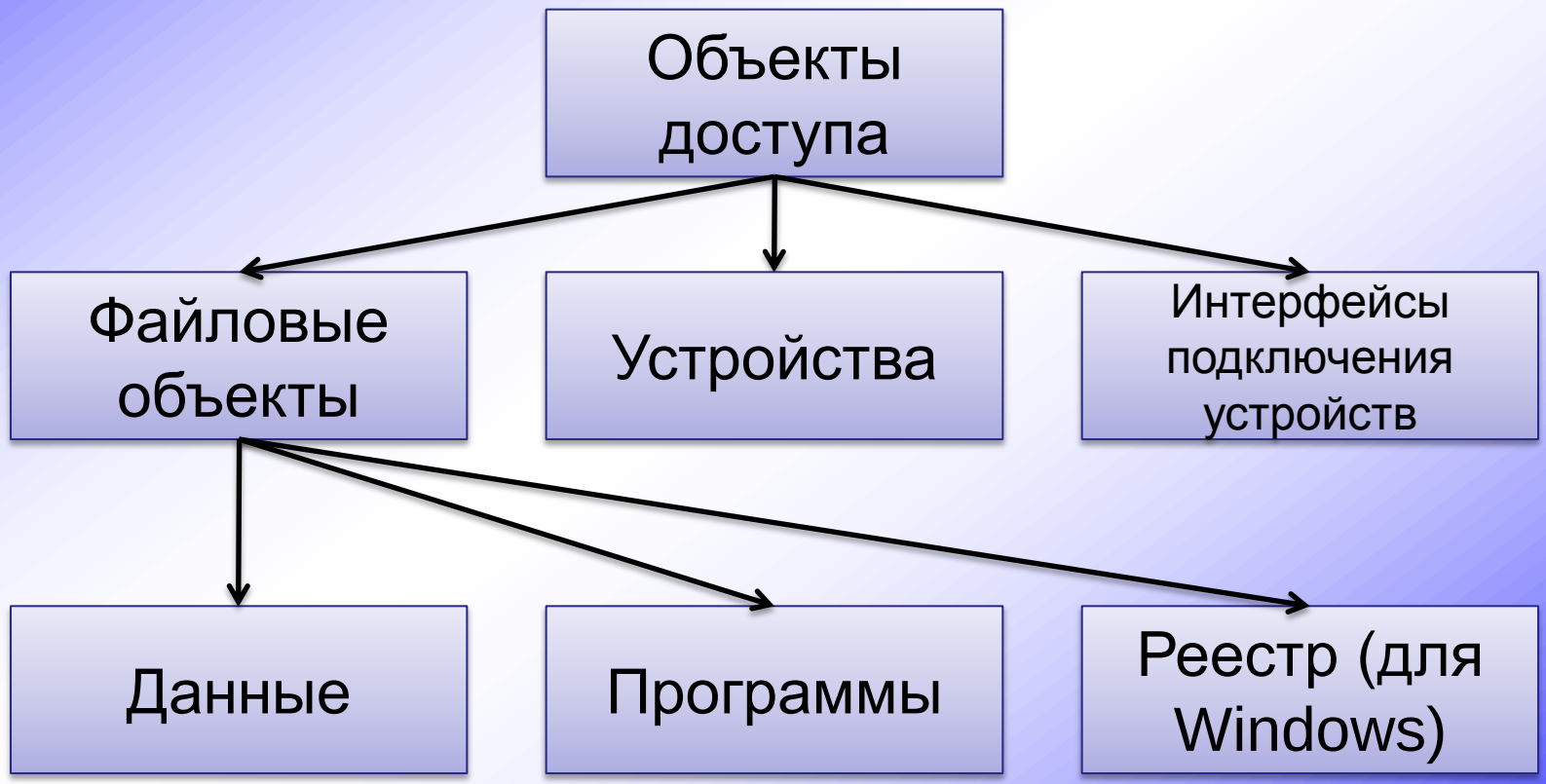
- Операционные системы обеспечивают безопасность информации только во время её обработки.
- При хранении информации ОС не может обеспечить безопасность, т.к. она отключена.
- При доставке информации ОС не может обеспечить безопасность, т.к. информация выходит за пределы ОС.

Ресурсы операционной системы как объекты угроз

Защищаемые объекты в ОС

- При работе ОС необходимо защищать ресурсы, к которым может осуществить доступ пользователь или запущенный им процесс.
- Должны учитываться объекты, хранящие защищаемую информацию, и объекты, позволяющие передать защищаемую информацию на другой носитель.
- Рассматриваются только локальные ресурсы.

Классификация защищаемых объектов



Файловые объекты

- Файлы с данными (файлы и каталоги).
- Исполняемые файлы (программы).
- Файлы с настройками операционной системы (для семейства Windows NT – реестр).

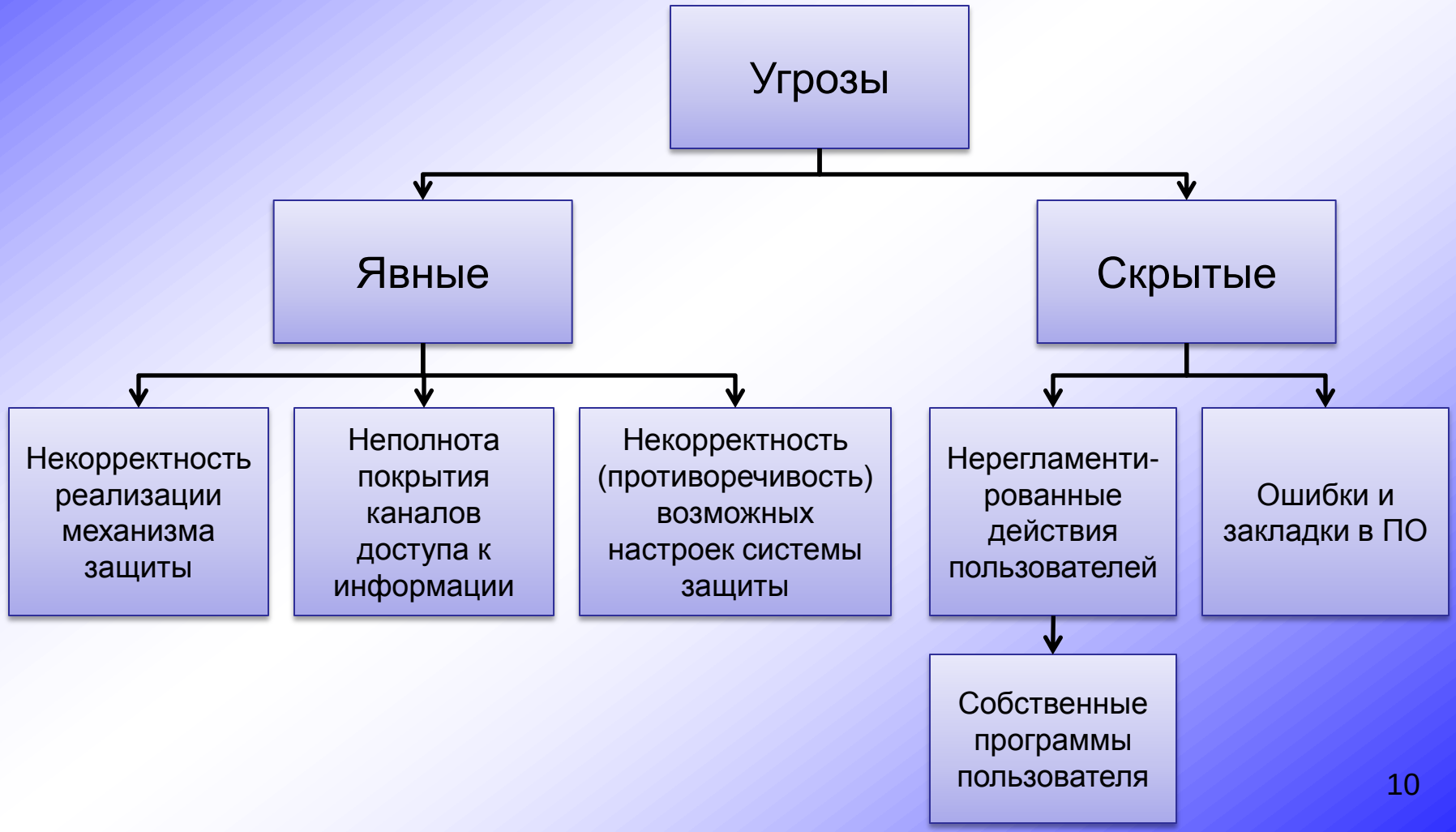
Интерфейсы подключения устройств

- USB-порты.
- LPT, COM-порты.
- ИК-порты и др.

Устройства ввода/вывода

- Жёсткие диски.
- Устройства с отчуждаемыми носителями информации (CD-, DVD-привод, кардридер и др.).
- Съёмные носители информации (USB-накопители, CD-, DVD-диски и др.).
- Остальные устройства ввода-вывода (принтеры, WiFi-адаптеры и др.).

Классификация угроз по способу их осуществления



Классификация объектов угроз

- Информационные ресурсы защищаемого объекта (локальные и сетевые): ОС (вход в систему), файловые объекты и др.
- Программные средства защищаемого объекта: системные утилиты, прикладные приложения и ПО системы защиты.
- Настройки программного обеспечения: настройки системного, прикладного ПО и средств защиты.
- Аппаратные средства защищаемого объекта: оборудование компьютера и системы защиты.

Требования к безопасности операционных систем

Основные подходы к обеспечению компьютерной безопасности

- Использование только встроенных в операционную систему и приложения средств защиты.
- Применение, наряду со встроенными, дополнительных механизмов защиты (программных или программно-аппаратных комплексов).

Требования к безопасности операционных систем

- Руководящий документ ГТК России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».
- Базовый профиль защиты, определяющий требования безопасности для операционных систем общего назначения, которые удовлетворяют третьему оценочному уровню доверия к безопасности (ОУД 3).

Функциональные требования безопасности

- Аудит безопасности.
- Защита данных пользователя.
- Идентификация и аутентификация.
- Управление безопасностью.
- Защита функций безопасности объекта оценки (ФБО).
- Использование ресурсов.
- Доступ к объекту оценки (ОО).
- Доверенный маршрут/канал.

Класс «Аудит безопасности»

- Аудит безопасности включает в себя распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности.
- Записи аудита, получаемые в результате, могут быть проанализированы, чтобы определить, какие действия, относящиеся к безопасности, происходили, и кто из пользователей за них отвечает.

Семейства класса «Аудит безопасности»

- Автоматическая реакция аудита безопасности.
- Генерация данных аудита безопасности.
- Просмотр аудита безопасности.
- Выбор событий аудита безопасности.
- Хранение данных аудита безопасности.

Класс «Защита данных пользователя»

Содержит семейства, определяющие требования к функциям безопасности ОО и политикам функций безопасности ОО, связанным с защитой данных пользователя.

Семейства класса:

- политика управления доступом;
- функции управления доступом;
- защита остаточной информации.

Класс «Идентификация и аутентификация»

Семейства этого класса связаны с определением и верификацией идентификаторов пользователей, определением их полномочий на взаимодействие с ОО, а также с правильной ассоциацией атрибутов безопасности (таких, как идентификатор, группы, роли, уровни безопасности или целостности) с каждым уполномоченным пользователем.

Семейства класса «Идентификация и аутентификация»

- Отказы аутентификации.
- Определение атрибутов пользователя.
- Спецификация секретов.
- Аутентификация пользователя.
- Идентификация пользователя.
- Связывание пользователь-субъект.

Класс «Управление безопасностью»

Предназначен для спецификации управления некоторыми аспектами ФБО: атрибутами безопасности, данными и отдельными функциями. Могут быть установлены различные роли управления, а также определено их взаимодействие, например распределение обязанностей.

Класс позволяет решать следующие задачи:

- управление данными ФБО, которые включают в себя, например, предупреждающие сообщения;
- управление атрибутами безопасности, которые включают в себя, например, списки управления доступом и перечни возможностей;
- управление функциями из числа ФБО, которое включает в себя, например, выбор функций, а также правил или условий, влияющих на режим выполнения ФБО;
- определение ролей безопасности.

Семейства класса «Управление безопасностью»

- Управление отдельными функциями ФБО.
- Управление атрибутами безопасности.
- Управление данными ФБО.
- Отмена.
- Срок действия атрибута безопасности.
- Роли управления безопасностью.

Класс «Защита ФБО»

Класс содержит семейства функциональных требований, которые связаны с целостностью и управлением механизмами, реализованными в ФБО, не завися при этом от особенностей политики безопасности объекта оценки (ПБО), а также с целостностью данных ФБО, не завися от специфического содержания данных ПБО. Класс нацелен на защиту данных ФБО. Фактически, компоненты из класса необходимы для обеспечения требований невозможности нарушения и обхода политик ФБ данного ОО.

Семейства класса «Защита ФБО»

- Тестирование базовой абстрактной машины.
- Передача данных ФБО в пределах ОО.
- Надёжное восстановление.
- Посредничество при обращениях.
- Разделение домена.
- Метки времени.
- Согласованность данных ФБО при дублировании в пределах ОО.
- Самотестирование ФБО.

Класс «Использование ресурсов»

- Класс поддерживает доступность требуемых ресурсов, таких как вычислительные возможности и/или объем памяти.
- Семейство класса: распределение ресурсов.

Класс «Доступ к объекту оценки»

Класс определяет функциональные требования к управлению открытием сеанса пользователя.

Семейства класса:

- блокирование сеанса;
- предупреждения перед предоставлением доступа к ОО;
- история доступа к ОО.

Класс «Доверенный маршрут/канал»

- Семейство: доверенный маршрут.
- Доверенный маршрут предоставляет пользователям средства для выполнения функций путем обеспечения прямого взаимодействия с ФБО. Доверенный маршрут обычно желателен при начальной идентификации и/или аутентификации пользователя, но может быть также применен на протяжении всего сеанса пользователя. Обмены по доверенному маршруту могут быть инициированы пользователем или ФБО. Гарантируется, что ответы пользователя с применением доверенного маршрута будут защищены от модификации или раскрытия недоверенными приложениями.

Руководящие документы по защите от несанкционированного доступа

- Руководящий документ ГТК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
- Руководящий документ ГТК «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации».

Группы классов защищённости АС от НСД к информации

- Третья группа включает автоматизированные системы (АС), в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.
- Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.
- Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Подсистемы системы защиты информации от НСД

- Подсистема управления доступом.
- Подсистема регистрации и учёта.
- Криптографическая подсистема.
- Подсистема обеспечения целостности.

Подсистема управления доступом

Требования	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
к программам	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+

" - " - нет требований к данному классу;
" + " - есть требования к данному классу.

Подсистема регистрации и учёта

Требования	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
2.1. Регистрация и учёт:									
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
запуска (завершения) программ и процессов	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+

Подсистема регистрации и учёта

Требования	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
2.1. Регистрация и учёт (окончание):									
изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2. Учёт носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+

Группы классов защищённости СВТ от НСД к информации

- Первая группа содержит только один седьмой класс (Седьмой класс присваивают средствам вычислительной техники (СВТ), к которым предъявлялись требования по защите от НСД к информации, но при оценке защищённость СВТ оказалась ниже уровня требований шестого класса).
- Вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы.
- Третья группа характеризуется мандатной защитой и содержит четвёртый, третий и второй классы.
- Четвёртая группа характеризуется верифицированной защитой и содержит только первый класс.

Показатели по классам защищённости СВТ

Наименование показателя	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надёжное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=

"-" – нет требований к данному классу;
"+" – новые или дополнительные требования,
"=" – требования совпадают с требованиями к СВТ предыдущего класса.

Работа с информацией, отнесённой к секретной

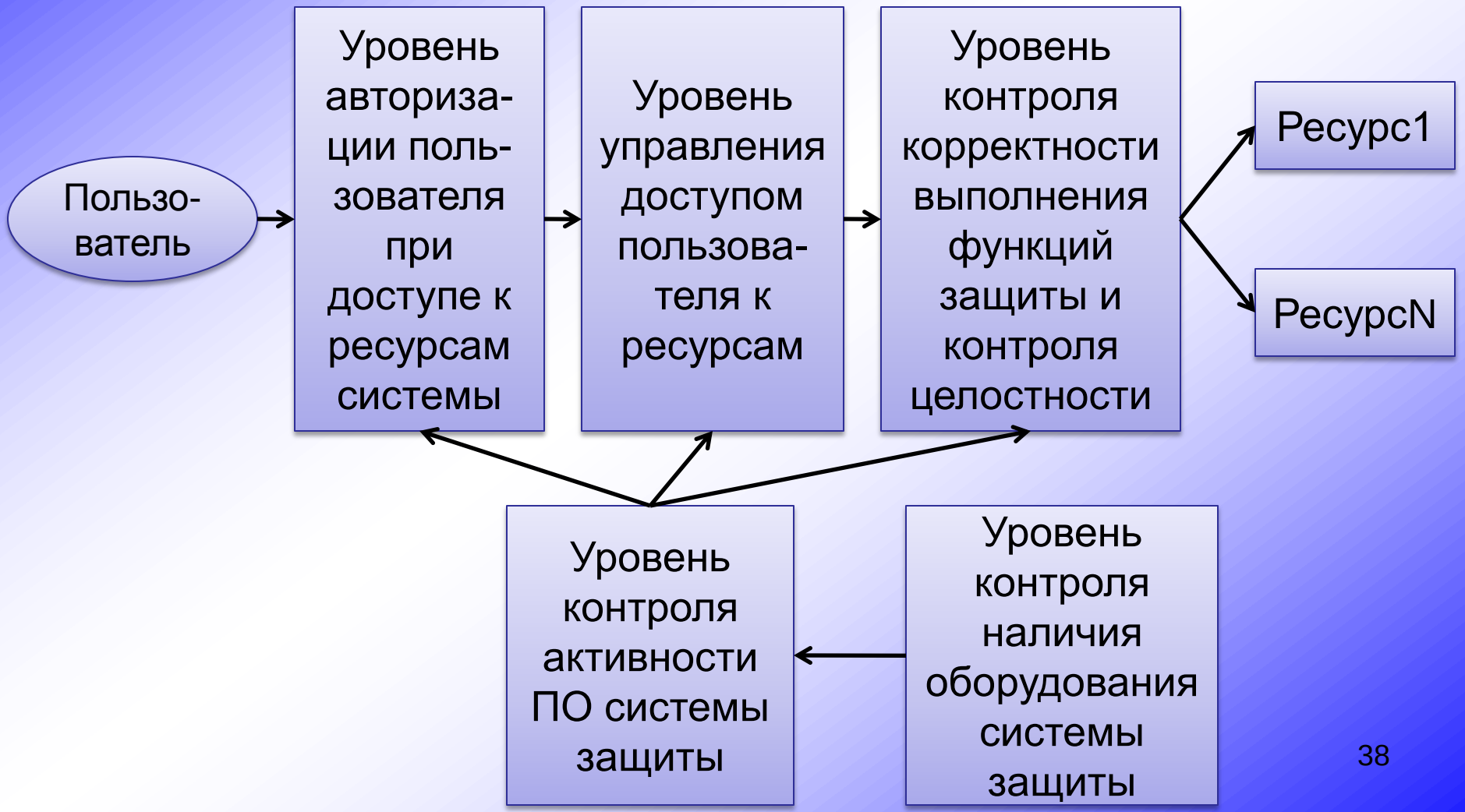
При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться на классы защищённости АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

- не ниже 4 класса - для класса защищённости АС 1В;
- не ниже 3 класса - для класса защищённости АС 1Б;
- не ниже 2 класса - для класса защищённости АС 1А.

Основные группы механизмов защиты

- Механизмы авторизации пользователей.
- Механизмы управления доступом пользователей к ресурсам.
- Механизмы контроля целостности.
- Механизмы регистрации (аудита).

Модель системы защиты информации



Уровень авторизации пользователя при доступе к ресурсам системы

- Проверка учётных параметров пользователя при доступе в систему и к системе защиты.
- Запуск приложений после авторизации.

Уровень управления доступом пользователя к ресурсам

- Реализация разграничительной схемы доступа пользователя к ресурсам защищаемого объекта.
- Реализация политики администрирования.
- Локальные ресурсы: файловые объекты (разделы, каталоги, файлы), устройства со сменными носителями, отчуждаемые физические носители, порты, локальные принтеры, исполняемые файлы, настройки ОС, файлы настроек системы защиты, настройки приложений и т.д.
- Сетевые ресурсы: разделяемые сетевые ресурсы, протоколы, виртуальные каналы связи, сетевые принтеры, сетевые службы и приложения, их настройки

Уровень контроля корректности выполнения функций защиты и контроля целостности

- Фиксирование фактов использования злоумышленником ошибок и закладок в системном и прикладном ПО.
- Контроль целостности программ и данных (файловых объектов).

Уровень контроля активности ПО системы защиты

- Контроль активности системы защиты.
- Предотвращение возможности функционирования ОС при отключенной системе защиты.
- Реализации контроля: локальная (на аппаратном уровне), сетевая (удалённо администратором).

Уровень контроля наличия оборудования системы защиты

- Необходима в случае наличия аппаратной компоненты в системе защиты.
- Техническая защита от удаления аппаратной компоненты защиты.

Регистрация событий (аудит)

Регистрация (аудит) событий осуществляется каждым реализованным в системе механизмом защиты.

- Аудит первого уровня. Осуществляется уровнями авторизации и разграничения прав доступа. Происходит полный аудит правомерных и неправомерных действий пользователя. Получение накопленной информации по запросу.
- Аудит второго уровня. Осуществляется уровнем контроля корректности выполнения функций защиты и контроля целостности. Фиксируются только критичные факты НСД, связанные с преодолением злоумышленником механизмов защиты первых двух уровней. Получение информации в реальном времени.

Рассмотренные вопросы

- Существующие угрозы, классификация методов и способов их осуществления.
- Руководящие документы, в которых формулируются требования к средствам обеспечения безопасности.
- Модель системы защиты информации.

Всем спасибо – все свободны,

если нет вопросов