**Вопросы по 5-ому семестру.**

Вопрос 1.Какие технологии информационной защиты необходимо использовать чтобы обеспечить надежную защиту ресурсов информационной системы?

* *анализ угроз информационной безопасности* информационной системы;
* *разработка единой политики информационной безопасности* организации;
* *комплексный многоуровневый подход к обеспечению информационной безопасности*, обеспечивающий рациональное сочетание технологий и средств информационной защиты;
* *криптографическая защита данных* для обеспечения конфиденциальности, целостности и подлинности информации;
* *поддержка инфраструктуры управления открытыми ключами PKI;*
* *технологии аутентификации* для проверки подлинности пользователей и объектов сети путем применения одноразовых паролей, токенов (смарт-карт, USB-токенов) и других средств аутентификации;
* *управление доступом на уровне пользователей* и защита от несанкционированного доступа к информации;
* *технологии межсетевых экранов* для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
* *технологии виртуальных защищенных каналов и сетей VPN* для защиты информации, передаваемой по открытым каналам связи;
* *технологии обнаружения и предотвращения вторжений в ИС;*
* *технологии защиты от вредоносных программ и спама* с использованием комплексов антивирусной защиты;
* *обеспечение безопасности «облачных» вычислений;*
* *централизованное управление средствами информационной безопасности* на базе единой политики безопасности организации.

Вопрос 2. Что такое доступность, целостность и конфиденциальность?

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Доступность данных – работа пользователя с данными возможна только в том случае, если он имеет к ним доступ. Доступность является весьма важным элементом информационной безопасности. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – военными подразделениями, производством, транспортом.

Под целостностью подразумеваются актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Обеспечение целостности данных является одной из сложных задач защиты информации.

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной. Основным средством обеспечения конфиденциальности является использование криптографии.

Вопрос 3. Что такое угроза безопасности информации, ущерб безопасности, источник угрозы безопасности, уязвимость, атака?

Угроза (безопасности информации) – совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Такие факторы способны прямо или косвенно нанести ущерб безопасности ИС.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатываемой в системе (сети).

Источник угрозы безопасности информации – субъект (физическое лицо), материальный объект или физическое явление, являющиеся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и не связанные с деятельностью человека. Примерами могут служить удаление пользователем файла с важной информацией или пожар в здании соответственно. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Уязвимость информационной системы – свойство информационной системы, обусловливающее возможность реализации угрозы безопасности, обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, если в ИС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

*Атака* на компьютерную систему – это поиск и/или использование злоумышленником той или иной уязвимости системы. Иными словами, атака – это реализация угрозы безопасности.

Вопрос 4. Что такое защита информации, объект защиты, эффективность защиты информации, цель защиты информации, защита информации от утечки?

*Защита информации* – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

*Объект защиты* – информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

*Эффективность защиты информации* – степень соответствия результатов защиты информации поставленной цели.

*Цель защиты информации* – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

*Защита информации от утечки* – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к ней и от получения защищаемой информации злоумышленниками.

Вопрос 5. Что такое санкционированный и несанкционированный доступ к информации, права доступа?

Санкционированный доступ к информации – это доступ к информации, не нарушающий установленных правил разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (НСД) к информации характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Права доступа — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (информации, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации.

Права доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам (например, пользователям системы) над объектами данных. Для этого требуется некая система для предоставления субъектам различных прав доступа к объектам. Это система разграничения доступа субъектов к объектам, которая рассматривается в качестве главного средства защиты от несанкционированного доступа к информации или порче самой системы.

Вопрос 6. Что такое идентификация, аутентификация и авторизация?

*Идентификация субъекта* – это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть).

Следующим шагом взаимодействия системы с субъектом является аутентификация субъекта.

*Аутентификация субъекта* – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил.

После идентификации и аутентификации субъекта выполняют процедуру авторизации.

*Авторизация субъекта* – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Вопрос 7. Опишите угрозы безопасности операционной системы.

Операцио́нная систе́ма — комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем. В логической структуре типичной вычислительной системы операционная система занимает положение между устройствами с их микроархитектурой, машинным языком и, возможно, собственными (встроенными) микропрограммами (драйверами) — с одной стороны — и прикладными программами с другой.

Организация эффективной и надежной защиты операционной системы невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности операционной системы существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе. Например, если операционная система используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации.

Классификация угроз *по цели атаки*:

* несанкционированное чтение информации;
* несанкционированное изменение информации;
* несанкционированное уничтожение информации;
* полное или частичное разрушение операционной системы.

Классификация угроз *по принципу воздействия на операционную систему:*

* использование известных (легальных) каналов получения информации, например, угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно – разрешен доступ пользователю, которому, согласно политике безопасности, доступ должен быть запрещен;
* использование скрытых каналов получения информации, например, угроза использования злоумышленником недокументированных возможностей операционной системы;
* создание новых каналов получения информации с помощью программных закладок.

Классификация угроз *по типу используемой злоумышленником уязвимости защиты:*

* неадекватная политика безопасности, в том числе и ошибки администратора системы;
* ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые люки – случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
* ранее внедренная программная закладка.

Классификация угроз *по характеру воздействия на ОС:*

* активное воздействие – несанкционированные действия злоумышленника в системе;
* пассивное воздействие – несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Вопрос 8. Опишите типичные атаки на операционную систему.

* *сканирование файловой системы.* Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, который должен быть ему запрещен;
* *подбор пароля.* Существует несколько методов подбора паролей пользователей:
	+ тотальный перебор;
	+ тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;
	+ подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);
* *кража ключевой информации.* Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарткарта, Touch Memory и т. д.) может быть просто украден;
* *сборка мусора.* Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Злоумышленник восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;
* *превышение полномочий.* Злоумышленник, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя;
* *программные закладки.* Программные закладки, внедряемые в операционные системы, не имеют существенных отличий от других классов программных закладок;
* *жадные программы* – это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху операционной системы.

Вопрос 9. Какие административные меры применяются для защиты операционных систем?

Программно-аппаратные средства защиты операционной системы обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже надежная программно-аппаратная защита может давать сбои. Перечислим основные административные меры защиты.

1. *Постоянный контроль корректности функционирования операционной системы,* особенно ее подсистемы защиты. Такой контроль удобно организовать, если операционная система поддерживает автоматическую регистрацию наиболее важных событий (event logging) в специальном журнале.
2. *Организация и поддержание адекватной политики безопасности.* Политика безопасности ОС должна постоянно корректироваться, оперативно реагируя на попытки злоумышленников преодолеть защиту операционной системы, а также на изменения в конфигурации операционной системы, установку и удаление прикладных программ.
3. *Осведомление пользователей операционной системы* о необходимости соблюдения мер безопасности при работе с ОС и контроль за соблюдением этих мер.
4. *Регулярное создание и обновление резервных копий* программ и данных ОС.
5. *Постоянный контроль изменений в конфигурационных данных и политике безопасности ОС.*

Вопрос 10. На какие этапы можно разделить процесс формирования и поддержания адекватной политики безопасности (ПБ) для ОС?

1. *Анализ угроз.* Администратор операционной системы рассматривает возможные угрозы безопасности данного экземпляра ОС. Среди возможных угроз выделяются наиболее опасные, защите от которых нужно уделять максимум средств.
2. *Формирование требований к политике безопасности (ПБ).* Администратор определяет, какие средства и методы будут применяться для защиты от тех или иных угроз. Например, защиту от НСД к некоторому объекту ОС можно решать либо средствами разграничения доступа, либо криптографическими средствами, либо используя некоторую комбинацию этих средств.
3. *Формальное определение ПБ.* Администратор определяет, как конкретно должны выполняться требования, сформулированные на предыдущем этапе. Формулируются необходимые требования к конфигурации ОС, а также требования к конфигурации дополнительных пакетов защиты, если установка таких пакетов необходима. Результатом данного этапа является развернутый перечень настроек конфигурации ОС и дополнительных пакетов защиты с указанием того, в каких ситуациях какие настройки должны быть установлены.
4. *Претворение в жизнь ПБ.* Задачей данного этапа является приведение конфигурации ОС и дополнительных пакетов защиты в соответствие с политикой безопасности, формально определенной на предыдущем этапе.
5. *Поддержание и коррекция ПБ.* В задачу администратора на данном этапе входят контроль соблюдения политики безопасности и внесение в нее необходимых изменений по мере появления изменений в функционировании ОС.

Вопрос 11. Опишите основные функции подсистемы защиты операционной системы.

Подсистема защиты ОС выполняет следующие основные функции:

1. *Идентификация и аутентификация.* Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.
2. *Разграничение доступа.* Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.
3. *Аудит.* Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.
4. *Управление политикой безопасности.* Политика безопасности должна постоянно поддерживаться в адекватном состоянии, то есть должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в операционную систему.
5. *Криптографические функции.* Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.
6. *Сетевые функции.* Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе имеющих прямое отношение к защите информации.

Подсистема защиты обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями подсистемы защиты должен существовать четко определенный интерфейс, используемый при взаимодействии модулей для решения общих задач.

Ядро́ — центральная часть ОС, обеспечивающая приложениям координированный доступ к ресурсам компьютера, таким как процессорное время, память, внешнее аппаратное обеспечение, внешнее устройство ввода и вывода информации. Также обычно ядро предоставляет сервисы файловой системы и сетевых протоколов.

Вопрос 12. Каким требованиям должны удовлетворять правила разграничения доступа (ПРД)?

Разграничением доступа субъектов к объектам является совокупность правил, определяющая для каждой тройки субъект–объект–метод, разрешен ли доступ данного субъекта к данному объекту по данному методу.

*Субъектом доступа* называют любую сущность, способную инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа). Субъекта доступа называют суперпользователем, если он имеет возможность игнорировать правила разграничения доступа к объектам.

*Объектом доступа* называют любой элемент ОС, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Возможность доступа к объектам ОС определяется не только архитектурой операционной системы, но и текущей политикой безопасности. Под объектами доступа понимают, как ресурсы оборудования, так и программные ресурсы. В качестве примера ресурсов оборудования можно привести процессор, принтер, жесткие диски и ленты. Каждый объект имеет уникальное имя, отличающее его от других объектов в системе, и может быть доступен через хорошо определенные и значимые операции.

*Методом доступа к объекту* называется операция, определенная для объекта. Тип операции зависит от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а для файлов могут быть определены методы доступа «чтение», «запись » и «добавление» (дописывание информации в конец файла).

Требования к ПРД:

1. ПРД, принятые в операционной системе, должны соответствовать аналогичным правилам, принятым в организации, в которой установлена эта ОС. Иными словами, если согласно правилам организации, доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен.
2. ПРД не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ОС.
3. Любой объект доступа должен иметь владельца. Недопустимо присутствие ничейных объектов – объектов, не имеющих владельца.
4. Недопустимо присутствие недоступных объектов – объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа.
5. Недопустима утечка конфиденциальной информации.

Вопрос 13. Назовите две основные модели разграничения доступа (РД).

Существуют две основные модели разграничения доступа:

* избирательное (дискреционное) разграничение доступа;
* полномочное (мандатное) разграничение доступа.

При *избирательном РД*  (Discretionary Access Control) определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. Большинство операционных систем реализуют именно избирательное разграничение доступа.

*Полномочное РД* заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов.

Вопрос 14. Опишите систему правил избирательного (дискреционного) разграничение доступа (РД).

Система правил избирательного РД формулируется следующим образом.

1. Для любого объекта ОС существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой тройки субъект–объект–метод возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

Этот привилегированный пользователь не может игнорировать разграничение доступа к объектам. Например, в ОС типа Windows администратор для обращения к чужому объекту (принадлежащему другому субъекту) должен вначале объявить себя владельцем этого объекта, используя привилегию администратора объявлять себя владельцем любого объекта, затем дать себе необходимые права, и только после этого администратор может обратиться к объекту. Последнее требование введено для реализации механизма удаления потенциально недоступных объектов.

При создании объекта его владельцем назначается субъект, создавший данный объект. В дальнейшем субъект, обладающий необходимыми правами, может назначить объекту нового владельца.

При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя. Такое ограничение вводится для того, чтобы владелец объекта не мог отдать владение объектом другому субъекту и тем самым снять с себя ответственность за некорректные действия с объектом.

Вопрос 15. Опишите правила полномочного разграничение доступа (РД) с контролем информационных потоков.

Полномочное, или мандатное, РД (Mandatory Access Control, MAC) обычно применяется в совокупности с избирательным разграничением доступа. Рассмотрим именно такой случай.

Правила разграничения доступа в данной модели формулируются следующим образом:

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой четверки субъект–объект–метод–процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Вместе с тем в каждый момент времени возможность доступа определена однозначно. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.
5. В множестве объектов выделяется множество объектов полномочного разграничения доступа. Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен. Если объект не является объектом полномочного РД или несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа.
6. Каждый субъект доступа имеет уровень допуска. Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.
7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

– объект является объектом полномочного разграничения доступа;

– гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему;

– субъект открывает объект в режиме, допускающем чтение информации.

Это правило называют правилом NRU (Not Read Up – не читать выше).

1. Каждый процесс операционной системы имеет уровень конфиденциальности, равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования. Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.
2. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

– объект является объектом полномочного разграничения доступа;

– гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему;

– субъект собирается записывать в объект информацию.

Это правило разграничения доступа предотвращает утечку секретной информации. Это так называемое правило NWD (Not Write Down – не записывать ниже).

1. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:

– имеет доступ к объекту согласно правилу 7;

– обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

Вопрос 16.Что представляет собой аудит применительно к ОС?

Процедура аудита применительно к ОС заключается в регистрации в специальном журнале, называемом журналом аудита, или журналом безопасности, событий, которые могут представлять опасность для операционной системы. Пользователи системы, обладающие правом чтения журнала аудита, называются аудиторами.

Необходимость включения в защищенную операционную систему функций аудита обусловлена следующими обстоятельствами:

* *обнаружение попыток вторжения* является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;
* подсистема защиты ОС может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал аудита, сможет установить, что произошло при вводе пользователем неправильного пароля – ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20–30 раз – это явная попытка подбора пароля;
* администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом. Такую возможность обеспечивает журнал аудита;
* если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась. Журнал аудита может содержать всю необходимую информацию.

К числу событий, которые могут представлять опасность для операционной системы, обычно относят следующие:

* вход или выход из системы;
* операции с файлами (открыть, закрыть, переименовать, удалить);
* обращение к удаленной системе;
* смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Если фиксировать в журнале аудита все события, объем регистрационной информации будет расти слишком быстро, что затруднит ее эффективный анализ. Необходимо предусмотреть выборочное протоколирование как в отношении пользователей, так и в отношении событий.

Вопрос 17. Какие требования необходимо предъявлять к подсистеме аудита защищенной ОС?

Подсистема аудита операционной системы должна удовлетворять следующим требованиям:

1. Добавлять записи в журнал аудита может только операционная система. Если предоставить это право какому-то физическому пользователю, этот пользователь получит возможность компрометировать других пользователей, добавляя в журнал аудита соответствующие записи.
2. Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, в том числе и сама ОС.
3. Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией.
4. Очищать журнал аудита могут только пользователи-аудиторы. После очистки журнала в него автоматически вносится запись о том, что журнал аудита был очищен, с указанием времени очистки журнала и имени пользователя, очистившего журнал. Операционная система должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле.

Вопрос 18. Что собой представляет компонент «Управление учетными записями пользователей (UAC)» в операционной системе Windows?

*Управление учетными записями пользователей User Account Control(UAC)* создавалось для того, чтобы в системе можно было полноценно работать без прав администратора. В состав UAC входят несколько технологий: учетная запись защищенного администратора, запросы на повышение прав, виртуализация реестра, виртуализация файловой системы и уровни целостности Windows. Впервые управление учетными записями пользователя появилось в ОС Windows Vista. Однако частая выдача запросов UAC в Windows Vista приводила к тому, что пользователи ее отключали. Многие компоненты новых операционных систем были переработаны, чтобы уменьшить количество запросов UAC и обеспечить пользователям более комфортную работу. По сравнению с Windows Vista и Windows Server 2008, в операционных системах Windows 7 и Windows Server 2008 R2 появились следующие улучшения в функционале контроля учетных записей пользователей:

* увеличилось количество задач, которые может выполнять обычный пользователь без запроса подтверждения администратором;
* пользователю с правами администратора разрешается настраивать уровень UAC из Панели управления;
* существуют дополнительные настройки локальной политики безопасности, которые позволяют локальным администраторам изменять поведение сообщений UAC для локальных администраторов в режиме одобрения администратором;
* существуют дополнительные настройки локальной политики безопасности, которые позволяют локальным администраторам изменять поведение сообщений UAC для обычных пользователей.

 Многое из того, что в предыдущих версиях Windows требовало административных привилегий, в Windows 7 доступно обычным пользователям. Благодаря использованию для повседневных задач учетной записи со стандартными правами снижается риск, что вредоносное ПО установит нежелательную программу или внесет опасные изменения в систему.

В ОС Windows 7 можно выбрать тип уведомлений UAC и частоту их появления. Имеются четыре основных уровня:

* *«Уведомлять при установке программ или попытке внесения ими изменений, а также при изменении параметров Windows пользователем».* Это максимальный уровень контроля учетных записей;
* *«Уведомлять при установке программ или попытке внесения ими изменений».* Этот уровень используется по умолчанию;
* *«Уведомлять при попытке установки программ или попытке внесения ими изменений (не затемнять рабочий стол)».* Затемнение рабочего стола (так называемый безопасный рабочий стол, Secure Desktop) – это своего рода подтверждение подлинности окна UAC, позволяющее визуально отличить поддельные запросы UAC от настоящих;
* *«Не уведомлять ни при установке программ или попытке внесения ими изменений, ни при изменении параметров Windows пользователем».* Контроль учетных записей отключен. Использовать этот уровень не рекомендуется. Рекомендуется оставить значение по умолчанию – «Уведомлять при установке программ или попытке внесения ими изменений».

Указанные четыре основных уровня можно настроить в соответствующем разделе Центра поддержки.

Большинство программ и задач из состава Windows 7 работают со стандартными правами пользователя. Пользователи с правами администратора при входе в систему обладают административными привилегиями. Это позволяет им случайно выполнить или неосознанно разрешить выполнение какой-либо административной задачи. Когда пользователь пытается выполнить административную задачу, например установить новую программу или изменить некоторые параметры системы, сначала производится запрос подтверждения этого действия. Однако такой режим не обеспечивает того же уровня защиты, как и работа со стандартными правами. Этот режим не гарантирует, что вредоносное ПО, уже проникшее на клиентский компьютер, не сможет внедриться в программу, работающую с повышенными правами. Он также не гарантирует, что программа с повышенными правами не попытается совершить вредоносных действий.

Для выполнения повседневных задач пользователям рекомендуется использовать учетную запись с правами пользователя.

Вопрос 19. Что собой представляет технология BitLocker в операционной системе Windows?

BitLocker – это удобный и надежный вариант защиты данных. При применении BitLocker вся информация, размещенная на защищенном жестком диске, всегда находится только в зашифрованном виде. Процедура шифрования/дешифрования осуществляется автоматически при обращении к данным. Если шифрование BitLocker включено на дисках операционной системы, обычная загрузочная последовательность может быть приостановлена, пока не будут предоставлены необходимые учётные данные.

Для реализации защиты операционной системы Windows 7 необходима специальная организация жесткого диска. На нем должны существовать системный раздел, с которого осуществляется первичная загрузка компьютера, и раздел с файлами операционной системы. Зашифрован может быть только второй из них. Системный раздел должен оставаться открытым.

Для хранения ключей расшифрования допускается использовать USB-накопитель, однако с точки зрения безопасности целесообразно использовать доверенный платформенный модуль TPM для хранения ключей шифрования и предотвращения программных атак на целостность системы или хранящиеся на дисках данные. Это увеличивает надежность хранения критически важных данных. Если такого модуля в системе нет, BitLocker будет обеспечивать защиту данных, но проверка целостности системы проводиться не будет.

Для аутентификации пользователя в BitLocker может использоваться парольная защита или смарт-карта. Кроме того, есть возможность автоматической разблокировки закрытого жесткого диска при входе пользователя в систему.

Один из главных рисков, для устранения которых создана технология BitLocker, – риск утечки данных с утерянных или украденных компьютеров.

Если злоумышленник получает физический доступ к компьютеру, он может:

* войти в систему Windows 7 и скопировать файлы;
* перезагрузить клиентский компьютер под управлением другой ОС, после чего:
	+ – просмотреть имена файлов;
	+ – скопировать файлы;
	+ – считать содержимое файла гибернации или файла подкачки, где обнаружить открытый текст документов, с которыми велась работа.

Даже если файлы зашифрованы файловой системой EFS, небрежный пользователь может переместить или скопировать файл из защищённого расположения в незащищенное, так что данные будут представлены открытым текстом. Несведущий ИТ-персонал может забыть установить шифрование для скрытых папок, в которых приложения хранят резервные копии файлов, с которыми идет работа.

В целях преодоления указанных рисков следует включить шифрование BitLocker, а также требовать проверки целостности и подлинности загрузочных компонентов перед предоставлением доступа к зашифрованному системному диску.

Вопрос 20. Опишите технологию шифрования внешних устройств с помощью технологии BitLocker to Go.

С помощью BitLocker to Go пользователи могут шифровать данные на портативных носителях вроде внешних жестких дисков и USB-накопителей. В качестве алгоритма шифрования по умолчанию используется AES с длиной ключа 128 бит, а при необходимости можно увеличить ее до 256 бит.

Перед шифрованием данных BitLocker to Go может использовать алгоритм, называемый диффузором (diffuser), основной целью применения которого является получение сильно разнящихся шифрованных данных при незначительно отличающихся исходных. Применение диффузора существенно затрудняет взлом ключей или дешифровку. Данная опция по умолчанию включена. Обеспечиваемый уровень безопасности вполне достаточен не только для защиты личной переписки от любопытных знакомых, но и в корпоративной среде.

Важная задача централизованного управления при внедрении средств шифрования, а именно архивирование ключей восстановления, на случай утраты пользователем данных для доступа к зашифрованной информации успешно решена в Windows 7 – эта информация хранится в Active Directory.

Функция BitLocker to Go обеспечивает защиту данных на съемных дисках даже в том случае, если диск оказывается потерянным или украденным. Защита BitLocker To Go весьма надежна, и даже если у злоумышленника есть физический доступ к диску, это не значит, что у него есть доступ и к данным на этом диске.

Вопрос 21. Опишите систему шифрования файлов Encrypting File System (EFS) в ОС Windows.

Система шифрования файлов Encrypting File System (EFS) позволяет шифровать файлы и папки для защиты от несанкционированного доступа.

Она полностью встроена в файловую систему NTFS и совершенно прозрачна для приложений. Когда пользователь или программа обращаются к зашифрованному файлу, операционная система автоматически пытается получить ключ расшифрования, после чего выполняет шифрование и расшифрование от имени пользователя. Пользователи, имеющие доступ к ключам, могут работать с зашифрованными файлами так, словно они не зашифрованы, в то время как остальным пользователям доступ будет запрещен.

В ОС Windows 7 в архитектуре EFS появилась полная поддержка эллиптической криптографии (ECC). Благодаря этому EFS отвечает требованиям к шифрованию, предъявляемым стандартом Suite B Агентства национальной безопасности США, и пригодна для защиты секретной информации в государственных учреждениях.

Для максимальной защиты данных рекомендуется использовать и BitLocker, и EFS. Задача системы шифрования файлов EFS – предотвратить «вынос» конфиденциальных данных самими сотрудниками организации, а также защитить информацию, находящуюся на утерянных или украденных компьютерах.

Получив физический доступ к компьютеру с незашифрованными данными, злоумышленник может предпринять следующее:

* перезапустить компьютер и повысить свои полномочия до локального администратора, в результате чего получить доступ к данным пользователей;
* попытаться войти в систему компьютера с ОС Windows 7,чтобы скопировать все доступные данные на съемный диск, после чего отправить их по электронной почте или передать по FTP на удаленный сервер;
* перезапустить компьютер под управлением другой ОС, чтобы напрямую скопировать файлы с жесткого диска;
* перезапустить компьютер под управлением другой ОС и считать содержимое файла подкачки, где обнаружить открытый текст документов, с которыми велась работа;
* из простого любопытства сотрудник может просмотреть закрытые файлы, принадлежащие другим пользователям общего компьютера.

Для снижения описанных рисков разглашения данных можно использовать шифрование информации на жестком диске. Усовершенствования технологии EFS в ОС Windows 7 позволят при этом достичь следующих результатов:

* злоумышленник не сможет прочитать зашифрованные файлы, используя другую операционную систему, если у него не будет ключа расшифрования. Для повышения защиты такой ключ можно хранить на смарт-карте;
* злоумышленник не сможет добраться до пользовательских данных с помощью атаки подбора пароля, если ключ EFS, принадлежащий пользователю, хранится на смарт-карте или если вместе с EFS используется шифрование BitLocker, охраняющее хэш пароля и кэшированные учетные данные;
* злоумышленник не сможет получить доступ к конфиденциальным данным пользователя, если с помощью групповой политики включить обязательное шифрование папки «Документы»;
* использование EFS позволяет шифровать данные на нескольких дисках и общих сетевых папках;
* использование EFS позволяет защищать содержимое системного файла подкачки и кэша автономных файлов.

Вопрос 22. Что собой представляет брандмауэр Windows. Назначение брандмауэра.

Брандмауэр Windows 7 фильтрует как входящий, так и исходящий трафик, что обеспечивает защиту на случай непредвиденного поведения компонентов системы. Для упрощения настройки и уменьшения числа конфликтов с политиками в интерфейсе консоли брандмауэра Windows сведены средства фильтрования входящего и исходящего трафиков, а также параметры IPsec сервера и изоляции домена.

Брандмауэр Windows в режиме повышенной безопасности поддерживает следующие профили.

Профиль домена. Этот профиль вступает в силу, когда компьютер подключается к сети и проходит проверку подлинности на контроллере домена, которому принадлежит компьютер.

Общий профиль. Этот профиль по умолчанию применяется для компьютера, не подключенного к домену. Его параметры должны накладывать самые сильные ограничения, поскольку компьютер подключается к публичной сети, где безопасность нельзя гарантировать в той степени, что в контролируемой ИТ-среде.

Частный профиль. Этот профиль будет использоваться, только если пользователь с правами локального администратора назначит его сети, ранее использовавшей общий профиль. Делать это рекомендуется лишь для доверенных сетей.

В Windows 7 может быть несколько активных профилей, по одному на сетевой адаптер. Если разные сетевые адаптеры подключены к разным сетям, для каждого из них выбирается тип профиля, подходящий этой сети, – частный, общий или доменный.

Возможность работы в сети – непреложное условие успешности современного предприятия. И в то же время корпоративная сеть является основной целью различных атак. В целях обеспечения сохранности компьютеров и данных необходимо использовать средства защиты от связанных с сетевой работой угроз.

Наиболее часто встречающиеся угрозы перечислены ниже:

* + неизвестное лицо проводит успешную атаку на компьютер с целью получения административных привилегий;
	+ атакующий с помощью сканеров сети удаленно находит открытые порты и проводит атаку на них;
	+ троянская программа устанавливает неразрешенное подключение к компьютеру атакующего и передает закрытую деловую информацию;
	+ переносной компьютер подвергается сетевой атаке в то время, когда находится вне корпоративного брандмауэра;
	+ компьютеры внутренней сети подвергаются сетевой атаке со стороны зараженного компьютера, у которого есть доступ к внутренней сети;
	+ существует потенциальный риск шантажа, связанного c успешным проникновением на внутренние компьютеры.

Брандмауэр Windows 7 обеспечивает защиту клиентского компьютера сразу после установки ОС. Он блокирует большую часть незапрошенного сетевого трафика, пока иные правила не будут установлены администратором или групповой политикой. Брандмауэр Windows также позволяет фильтровать исходящий трафик, причем по умолчанию весь такой трафик разрешен. В режиме повышенной безопасности рекомендуется включить брандмауэр Windows для всех трех профилей.

Вопрос 23. Опишите модель управления безопасностью сети «Рабочая группа» при использовании ОС Windows.

Модель управления безопасностью «Рабочая группа» — самая примитивная. Она предназначена для использования в небольших одноранговых сетях (3–10 компьютеров) и основана на том, что каждый компьютер в сети с операционными системами Windows имеет свою собственную локальную базу данных учетных записей и с помощью этой локальной БД осуществляется управление доступом к ресурсам данного компьютера. Локальная БД учетных записей называется база данных SAM (Security Account Manager) и хранится в реестре операционной системы.

База данных SAM хранится в реестре (в ключе HKEY\_LOCAL\_MACHINE\SAM\SAM), доступ к которому запрещен по умолчанию даже администраторам. SAM-сервер реализован в виде DLL-библиотеки samsrv.dll, загружаемой lsass.exe. Программный интерфейс для доступа клиентов к серверу реализован в виде функций, содержащихся в DLL-библиотеке samlib.dll.

Базы данных SAM отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.

Вопрос 24. Опишите доменную модель безопасности в сетях Microsoft.

В доменной модели существует единая база данных служб каталогов Active Directory, доступная всем компьютерам сети. Для этого в сети устанавливаются специализированные серверы, называемые контроллерами домена, которые хранят на своих жестких дисках эту базу.

Контроллеры домена, они хранят доменную базу данных учетных записей (каждый контроллер хранит у себя свою собственную копию БД, но все изменения, производимые в БД на одном из серверов, реплицируются на остальные контроллеры).

В доменной модели управления безопасностью пользователь регистрируется на компьютере («входит в систему») со своей доменной учетной записью и, независимо от компьютера, на котором была выполнена регистрация, получает доступ к необходимым сетевым ресурсам. И нет необходимости на каждом компьютере создавать большое количество локальных учетных записей, все записи созданы однократно в доменной БД. И с помощью доменной базы данных осуществляется централизованное управление доступом к сетевым ресурсам независимо от количества компьютеров в сети.

Вопрос 25. Что такое Active Directory?

Active Directory («Активный каталог», AD) — службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Первоначально создавалась, как LDAP-совместимая реализация службы каталогов, однако, начиная с Windows Server 2008, включает возможности интеграции с другими службами авторизации, выполняя для них интегрирующую и объединяющую роль. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики. Хранит данные и настройки среды в централизованной базе данных. Сети Active Directory могут быть различного размера: от нескольких десятков до нескольких миллионов объектов.

Active Directory имеет иерархическую структуру, состоящую из объектов. Объекты разделяются на три основные категории: ресурсы (например, принтеры), службы (например, электронная почта) и учётные записи пользователей и компьютеров. Служба предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности.

Объекты могут быть хранилищами для других объектов (группы безопасности и распространения). Объект уникально определяется своим именем и имеет набор атрибутов — характеристик и данных, которые он может содержать; последние, в свою очередь, зависят от типа объекта. Атрибуты являются составляющей базой структуры объекта и определяются в схеме. Схема определяет, какие типы объектов могут существовать.

Сама схема состоит из двух типов объектов: объекты классов схемы и объекты атрибутов схемы. Один объект класса схемы определяет один тип объекта Active Directory (например, объект «Пользователь»), а один объект атрибута схемы определяет атрибут, который объект может иметь.

Каждый объект атрибута может быть использован в нескольких разных объектах классов схемы. Эти объекты называются объектами схемы (или метаданными) и позволяют изменять и дополнять схему, когда это необходимо и возможно. Однако каждый объект схемы является частью определений объектов, поэтому отключение или изменение этих объектов могут иметь серьёзные последствия, так как в результате этих действий будет изменена структура каталогов. Изменение объекта схемы автоматически распространяется в службе каталогов. Будучи однажды созданным, объект схемы не может быть удалён, он может быть только отключён. Обычно все изменения схемы тщательно планируются.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имён, но, в отличие от объекта, контейнер не обозначает ничего конкретного: он может содержать группу объектов или другие контейнеры.

Вопрос 26. Что такое LDAP?

LDAP (англ. Lightweight Directory Access Protocol — «облегчённый протокол доступа к каталогам») — протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (bind), поиска (search) и сравнения (compare), а также операции добавления, изменения или удаления записей. Обычно LDAP-сервер принимает входящие соединения на порт 389 по протоколам TCP или UDP. Для LDAP-сеансов, инкапсулированных в SSL, обычно используется порт 636.

Всякая запись в каталоге LDAP состоит из одного или нескольких атрибутов и обладает уникальным именем (DN — англ. Distinguished Name). Уникальное имя может выглядеть, например, следующим образом: «cn=Иван Петров,ou=Сотрудники,dc=example,dc=com». Уникальное имя состоит из одного или нескольких относительных уникальных имён (RDN — англ. Relative Distinguished Name), разделённых запятой. Относительное уникальное имя имеет вид ИмяАтрибута=значение. На одном уровне каталога не может существовать двух записей с одинаковыми относительными уникальными именами. В силу такой структуры уникального имени записи в каталоге LDAP можно легко представить в виде дерева.

Запись может состоять только из тех атрибутов, которые определены в описании класса записи (object class), которые, в свою очередь, объединены в схемы (schema). В схеме определено, какие атрибуты являются для данного класса обязательными, а какие — необязательными. Также схема определяет тип и правила сравнения атрибутов. Каждый атрибут записи может хранить несколько значений.

LDAP является широко используемым стандартом доступа к службам каталогов. Из свободно распространяемых открытых реализаций наиболее известен сервер OpenLDAP, из проприетарных — поддержка протокола имеется в Active Directory — службе каталогов от компании Microsoft, предназначенной для централизации управления сетями Windows.

Вопрос 27. Каковы функции контроллеров домена Active Directory?

Домен безопасности (security domain) - часть автоматизированной системы, которая реализует одни и те же политики безопасности.

Основной единицей системы безопасности Active Directory является домен. Домен формирует область административной ответственности. База данных домена содержит учетные записи пользователей, групп и компьютеров. Большая часть функций по управлению службой каталогов работает на уровне домена (аутентификация пользователей, управление доступом к ресурсам, управление службами, управление репликацией, политики безопасности).

Имена доменов Active Directory формируются по той же схеме, что и имена в пространстве имен DNS. И это не случайно. Служба DNS является средством поиска компонент домена — в первую очередь контроллеров домена.

*Контроллеры домена* — специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory. Основные функции контроллеров домена:

* **хранение БД Active Directory** (организация доступа к информации, содержащейся в каталоге, включая управление этой информацией и ее модификацию);
* **синхронизация изменений в AD** (изменения в базу данных AD могут быть внесены на любом из контроллеров домена, любые изменения, осуществляемые на одном из контроллеров, будут синхронизированы c копиями, хранящимися на других контроллерах);
* **аутентификация пользователей** (любой из контроллеров домена осуществляет проверку полномочий пользователей, регистрирующихся на клиентских системах).

Настоятельно рекомендуется в каждом домене устанавливать не менее двух контроллеров домена — во-первых, для защиты от потери БД Active Directory в случае выхода из строя какого-либо контроллера, во-вторых, для распределения нагрузки между контроллерами.

Вопрос 28. Опишите ключевые особенности ОС Astra Linux Special Edition по реализации требований безопасности информации.

* Мандатное разграничение доступа
* Изоляция модулей
* Очистка оперативной и внешней памяти и гарантированное удаление файлов
* Маркировка документов
* Регистрация событий
* Механизмы защиты информации в графической подсистеме
* Режим ограничения действий пользователя (режим "киоск")
* Защита адресного пространства процессов
* Механизм контроля замкнутости программной среды
* Контроль целостности
* Средства организации домена
* Защищенная реляционная СУБД
* Защищенный комплекс программ электронной почты
* Защищенный комплекс программ гипертекстовой обработки данных

Вопрос 29. В чем различие Astra Linux Common Edition (CE) и Astra Linux Special Edition (SE). Перечислите релизы Astra Linux Special Edition.

Astra Linux CEпредназначена для обеспечения функциональности современных компьютеров при решении широкого круга пользовательских задач.

Astra Linux SE предназначена для создания на ее основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию до степени секретности "совершенно секретно" включительно.

Релиз «Смоленск» операционной системы специального назначения Astra Linux SE предназначен для функционирования на средствах вычислительной техники с процессорной архитектурой х86-64.

Релиз «Новороссийск» предназначен для функционирования на мобильных и встраиваемых компьютерах с процессорной архитектурой ARM.

Архитектура ARM (от англ. Advanced RISC Machine — усовершенствованная RISC-машина) — семейство лицензируемых 32-битных и 64-битных микропроцессорных ядер разработки компании ARM Limited.

RISC (англ. reduced instruction set computer — «компьютер с сокращённым набором команд») — архитектура процессора, в котором быстродействие увеличивается за счёт упрощения инструкций, чтобы их декодирование было более простым, а время выполнения — меньшим.

Релиз «Мурманск» разработан для функционирования на мэйнфреймах IBM System Z.

IBM System z (более раннее название — IBM eServer zSeries) — бренд, созданный компанией IBM для обозначения линейки мейнфреймов.

Релиз «Севастополь» — дистрибутив Astra Linux SE, предназначенный для функционирования на настольных, мобильных и встраиваемых компьютерах с процессорной архитектурой MIPS.

MIPS (англ. Microprocessor without Interlocked Pipeline Stages, микропроцессор без состояний задержки конвейера) — микропроцессор, разработанный компанией MIPS Computer Systems (в настоящее время MIPS Technologies) в соответствии с концепцией проектирования процессоров RISC.

Релиз «Керчь» — дистрибутив Astra Linux SE, предназначенный для функционирования на высокопроизводительных серверах, базирующихся на платформах с процессорной архитектурой POWER.

*POWER — микропроцессорная архитектура с ограниченным набором команд (RISC), разработанная и развиваемая компанией IBM. Название позже было расшифровано как Performance Optimization With Enhanced RISC (оптимизация производительности на базе расширенной архитектуры RISC).*

Релиз «Ленинград» — дистрибутив Astra Linux SE, предназначенный для работы на вычислительных комплексах «Эльбрус».

Вопрос 30. Опишите модель контроля и управления доступом в ОС Astra Linux Special Edition (SE).

Вместо системы принудительного контроля доступа SELinux, в Astra Linux Special Edition используется запатентованная мандатная сущностно-ролевая ДП-модель управления доступом и информационными потокам (МРОСЛ ДП-модель), которая лишена недостатков модели Белла — Лападулы (деклассификация, нарушение логики доступа к данным при обработке потока информации в распределённой среде) и содержит дополнительные способы разграничения доступа, например, два уровня целостности системы.

*МРОСЛ ДП-модель — мандатная сущностно-ролевая ДП-модель. ДП-модель — модель логического управления доступом «Д» и информационными потоками «П».*

В отличие от классической модели мандатного управления доступом, в МРОСЛ ДП-модели дополнительно к мандатному управлению доступом реализован мандатный контроль целостности дистрибутива и файловой системы (препятствующий доступу к защищаемой информации скомпрометированными субъектами после перехвата управления и повышения привилегий (получения административных прав), предусмотрено ролевое управление доступом, наличие иерархии сущностей и применено противодействие запрещённым потокам по памяти и по времени.

В настоящее время используемая в Astra Linux Special Edition модель разграничения доступа является единственной практически реализованной моделью, не основанной на SELinux, в российских реализациях операционных систем на базе Linux.

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.

SELinux был разработан Агентством национальной безопасности США, и затем его исходные коды были представлены для скачивания.

Вопрос 31. В чем заключаются особенности организации домена ALD?

Домен Astra Linux Directory (ALD) представляет собой набор средств для организации работы пользователей в локально вычислительной сети (ЛВС) на платформе ОС СН В основу положен доменный принцип построения ЛВС, при котором все логически связанные сетевые ресурсы и пользователи объединяются в единую систему идентификации и аутентификации с централизованным управлением политикой безопасности в соответствии с правилами мандатного разграничения доступа информации При этом пользователь получает возможность взаимодействия как с другими пользователями сети, так и с сетевыми ресурсами

Система управления доменом ALD построена на технологиях LDAP, Kerberos 5, CIFS и интегрирована со средствами защиты информации от НСД из состава ОС СН Система управления доменом ALD обеспечивает сквозную аутентификацию для входа в защищенную серверную группу и автоматическую настройку всех необходимых файлов конфигурации служб, а также предоставляет удобный интерфейс администрирования

Вопрос 32. Опишите модель информационной безопасности «КЦД»

Согласно модели «КЦД» все возможные нарушения информационной безопасности всегда могут быть отнесены по меньшей мере к одной из трех групп: нарушения конфиденциальности, нарушения целостности или нарушения доступности

Информационная система находится в состоянии безопасности, если она защищена от нарушений конфиденциальности, целостности и доступности, где:

1. **конфиденциальность (confidentiality)** — это состояние ИС, при котором информационные ресурсы доступны только тем пользователям, которым этот доступ разрешен;

2. **целостность (integrity)** — это состояние системы, при котором информация, хранящаяся и обрабатываемая этой И С, а также процедуры обработки информации не могут быть изменены, удалены или дополнены неавторизованным образом;

3. **доступность (availability)** — это состояние системы, при котором услуги, оказываемые системой, могут гарантированно и с приемлемой задержкой быть предоставлены пользователям, имеющим на это право.

Вопрос 33. Опишите модель информационной безопасности «Гексада Паркера»

Одной из наиболее популярных альтернатив триаде КЦД является так называемая гексада Паркера (Parkerian Hexad), в которой определено шесть базовых видов нарушений, в число которых, помимо нарушений конфиденциальности, доступности и целостности, входят еще три вида нарушений: аутентичности, владения и полезности.

**Аутентичность (authenticity)** — это состояние системы, при котором пользователь не может выдать себя за другого, а документ всегда имеет достоверную информацию о его источнике (авторе). Из этого определения видно, что аутентичность является аналогом неотказуемости.

**Владение (possession)** — это состояние системы, при котором физический контроль над устройством или другой средой хранения информации предоставляется только тем, кто имеет на это право.

**Полезность (utility)** — это такое состояние Информационной Системы, при котором обеспечивается удобство практического использования как собственно информации, так и связанных с ее обработкой и поддержкой процедур. В безопасной системе меры, предпринимаемые для защиты системы, не должны неприемлемо усложнять работу сотрудников, иначе они будут воспринимать их как помеху и пытаться при всякой возможности их обойти.

Российский государственный стандарт ГОСТ 13335-1:2006 дает определение информационной безопасности на основе гексады Паркера:

Вопрос 34. Опишите модель информационной безопасности «STRIDE»

STRIDE - это модель классификации угроз, разработанная Microsoft для анализа угроз компьютерной безопасности . Он предоставляет мнемонику для угроз безопасности в шести категориях.

STRIDE - это аббревиатура от следующих англоязычных названий типов нарушений безопасности:

**Spoofing** — Подмена;
**Tampering** — Изменение данных;
**Repudiation** — Отказ от ответственности;
**Information disclosure** — разглашения сведений;
**Denial of service** -отказ в обслуживании;
**Elevation of privilege** — захват привилегий.

В соответствии с этой моделью ИС находится в безопасности, если она защищена от следующих типов нарушений: подмены данных, изменения данных, отказа от ответственности, разглашения сведений, отказа в обслуживании, захвата привилегий.

**Подмена данных (spoofing)** — это такое нарушение, при котором пользователь или другой субъект ИС путем подмены данных, например IP-адреса отправителя, успешно выдает себя за другого, получая таким образом возможность нанесения вреда системе.

**Изменение (tampering)** означает нарушение целостности.

**Отказ от ответственности (repudiation)** представляет собой негативную форму уже рассмотренного нами свойства **неотказуемости (non-repudiation).**

**Разглашение сведений (information disclosure)** — это нарушение конфиденциальности.

**Отказ в обслуживании (denial of service)** касается нарушения доступности.

**Захват привилегий (elevation of privilege)** заключается в том, что пользователь или другой субъект Информационной Системы несанкционированным образом повышает свои полномочия в системе, в частности незаконное присвоение злоумышленником прав сетевого администратора снимает практически все защитные барьеры на его пути.

Вопрос 35. Что такое уязвимость ИС? Какие типы уязвимостей существуют?

**Уязвимость** **(vulnerability)** — это слабое звено информационной системы, которое, став известным злоумышленнику, может позволить ему нарушить ее безопасность.

Уязвимостями являются, например, ошибка в программе, примитивный пароль, неправильное назначение прав доступа к файлу с важными данными и множество других дефектов в разработке, эксплуатации или настройке системы.

Уязвимости системы могут быть скрытыми, то есть еще не обнаруженными, известными, но только теоретически, или же общеизвестными и активно используемыми злоумышленниками. Для общеизвестных уязвимостей в программных продуктах производители регулярно выпускают исправления, называемые патчами (patch — заплатка).

Многие из этих исправлений направлены на устранение уязвимостей. Однако к этой рутинной процедуре — регулярному внесению исправлений — не все и не всегда относятся с должным вниманием, из-за этого общеизвестные, но неисправленные ошибки в программном обеспечении являются одним из самых распространенных типов уязвимостей.

Другим типом уязвимостей, которыми часто пользуются злоумышленники, являются ошибки в конфигурировании программных и аппаратных средств. Например, имена «администратор» и «гость», установленные по умолчанию во многих ОС, могут облегчить злоумышленникам доступ к системе, поэтому они должны быть сразу при начальном конфигурировании ОС заменены другими, менее очевидными именами. С этой же целью администратор должен настроить подсистему интерактивного входа на то, чтобы она не показывала последнее имя пользователя, систему аудита — чтобы фиксировала все успешные и неуспешные попытки входа пользователей, а также выполнить другие столь же простые, но необходимые настройки.

Вопрос 36. Каким образом осуществляется поиск уязвимостей?

**Уязвимость** **(vulnerability)** — это слабое звено информационной системы, которое, став известным злоумышленнику, может позволить ему нарушить ее безопасность.

Поиск уязвимостей — важная часть задачи обеспечения безопасности. Эта работа включает в себя регулярное тестирование системы. В любой момент времени для любой системы можно указать множество различных видов уязвимостей, например, для операционных систем и приложений новые уязвимости появляются чуть ли не каждый день; выявлять их вручную — задача очень трудоемкая. Поэтому для автоматизации поиска уязвимостей используют различные программные инструменты — средства сканирования уязвимостей, такие, например, как Positive Technologies XSpider, Nessus и др.

Проект Nessus был основан в 1998. Первоначально являлся программным обеспечением с открытым исходным кодом. В октябре 2005 года компания Tenable Network Security приняла решение закрыть исходный код приложения и сделать его проприетарным. Исходный код Nessus 2 послужил основой проекта открытого сканера уязвимостей OpenVAS.

Сканирование заключается в последовательном (адрес за адресом узла, или номер за номером порта, или идентификатор за идентификатором сетевого соединения) направлении запросов целевой системе. Затем на основании полученных ответов генерируется «информационный отпечаток» и, наконец, сравнением «отпечатка» с записями в базе данных выполняется идентификация уязвимости.