Группа	**324**
Дата	**28.02.2025**
Время	**11.50 – 13.10**
Наименование УД	**ОП 09. Стандартизация, сертификация и техническое документирование**
Ф.И.О. преподавателя	**Горлачева Е.Н.**
Обратная связь	**e-meil: gorlachevaen@yandex.ru**
Основная литература	
Задание	Изучите материал лекции. В рабочей тетради запишите дату, тему занятия. Ответьте на контрольные вопросы. Сфотографируйте свою работу, пришлите фото на почту
Тема	**Стандарты и спецификации в области информационной безопасности.** Стандарты и спецификации в области информационной безопасности Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин. Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно. Отмеченная роль стандартов зафиксирована в основных понятиях закона РФ "О техническом регулировании" от 27 декабря 2002 года под номером 184-ФЗ (принят Государственной Думой 15 декабря 2002 года): стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения; стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг. Примечательно также, что в число принципов стандартизации, провозглашенных в статье 12 упомянутого закона, входит принцип применения международного стандарта как основы разработки национального, за исключением случаев, если "такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения". С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. Мы приступаем к обзору стандартов и спецификаций двух разных видов: • оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности; • технических спецификаций, регламентирующих различные аспекты реализации средств защиты. Важно отметить, что между эти видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры. Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем". Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был

впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия оценивается по двум основным критериям.

1. Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности – это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

2. Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Основное назначение доверенной вычислительной базы – выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности – это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, – нет.

Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности – в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Обычный способ идентификации – ввод имени пользователя при входе в систему.

	Стандартное средство проверки подлинности (аутентификации) пользователя – пароль. Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы. Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы. Британский стандарт BS 7799 "Управление информационной безопасностью. Практические правила", полезный для руководителей организаций и лиц, отвечающих за информационную безопасность, без сколько-нибудь существенных изменений воспроизведен в международном стандарте ISO/IEC 17799.
Контрольный тест	1. Какова роль стандартов информационной безопасности? 2. Назовите международные стандарты информационной безопасности. Какие вопросы они рассматривают? 3. Какие Российские стандарты регулируют информационную безопасность? 4. Перечислите основополагающие документы по информационной безопасности