Информационная безопасность

Лекция 7 Экспортный контроль

В. М. Куприянов, Национальный центр ИНИС МАГАТЭ, НИЯУ МИФИ

НЦ ИНИС МИФИ

Литература

Основная литература для изучения дисциплины:

- Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности.- М.: Горячая линия – Телеком, 2006.
- Петраков А.В. Основы практической защиты информации.- М.: Радио и связь, 2001.
- Шумский А.А., Шелупанов А.А. Системный анализ в защите информации.- М.: Гелиос АРВ, 2005.
- Герасименко В.А., Малюк А.А. Основы защиты информации.- М.: Инкомбук, 1997.
- Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.- М.: Энергоатомиздат, 1994.
- Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации.- Орел: ОВИПС, 2000.

Требования безопасности к информационным системам

- Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому этот стандарт очень часто называют "Общими критериями".
- "Общие критерии" являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.
- "Общие критерии" содержат два основных вида требований безопасности:
- **функциональные** – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия** – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.
- В отличие от "Оранжевой книги", "Общие критерии" не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.
- Очень важно, что безопасность в "Общих критериях" рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Жизненный цикл продукта

Жизненный цикл защиты

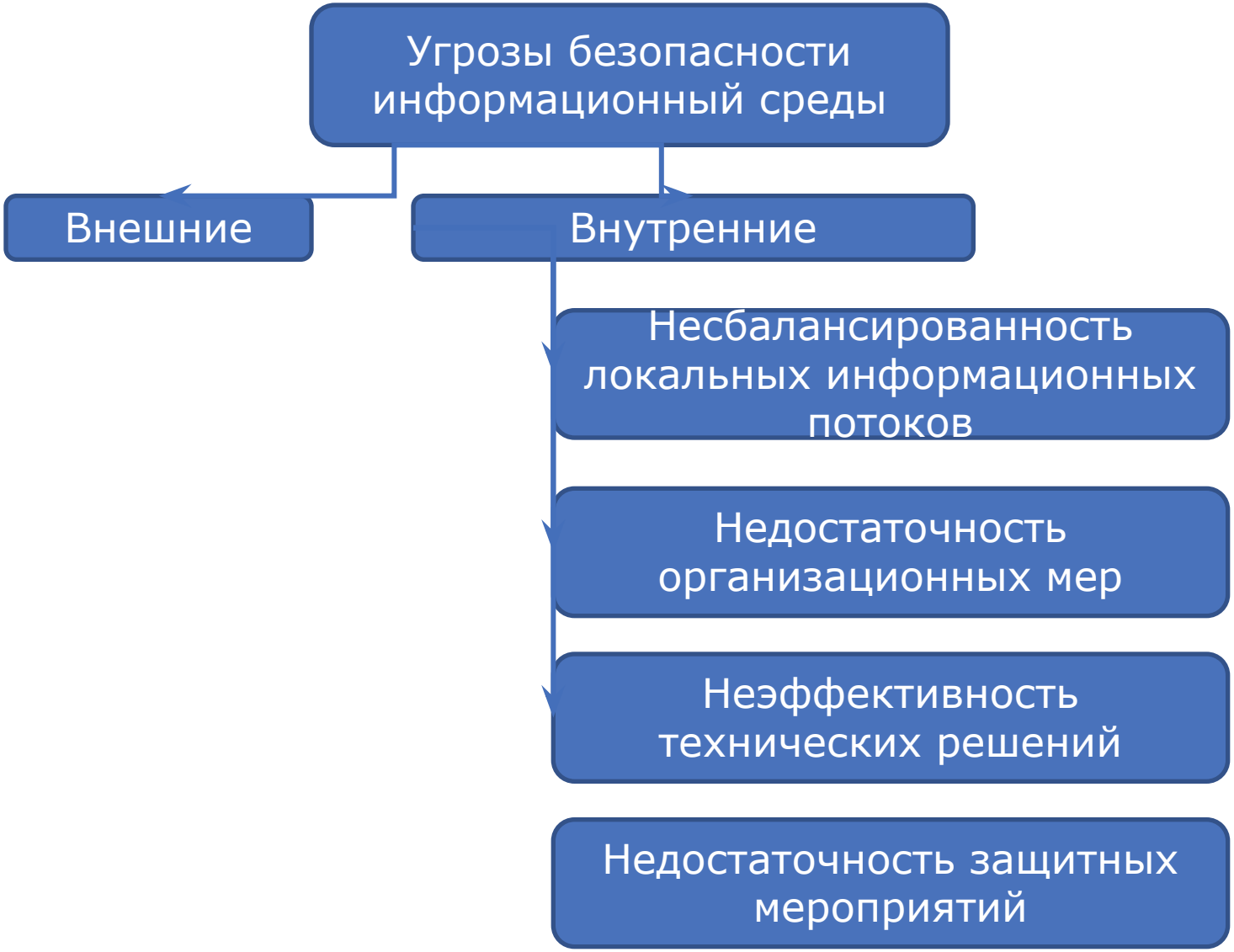
ОБЩИЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Если в результате проведенной оценки выясняется, что та или иная информация нуждается в защите, — необходимо принять меры по ее защите. Для этого необходимо предотвратить или значительно усложнить хищение информации и довести до сведения всех лиц, имеющих к ней доступ сведения о важности конкретной информации и мерах наказания за ее разглашение.

Целями защиты информации являются :

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

Оценка уязвимостей (включая оценку стойкости функций безопасности)



ОЦЕНКА УЯЗВИМОСТИ ИНФОРМАЦИИ

Для того чтобы обеспечить эффективную защиту интеллектуальной собственности, необходимо провести ее анализ. Требуется, во-первых, определить потенциальную ценность информационной собственности, во-вторых, оценить ее уязвимость (устойчивость к средствам разведки или поражения) и, в-третьих, спрогнозировать возможные угрозы. Определение потенциальной ценности информации обезопасит наиболее важные секреты, утечка которых способна нанести ущерб, значительно превышающий возможные затраты на их защиту.

При этом важно установить :

- какая информация нуждается в защите?
- кого она может заинтересовать?
- какие элементы информации наиболее ценны?
- каков “срок жизни” этих средств?
- во что обойдется их защита?

Оценка уязвимости информации дает возможность выявить характерные особенности и недостатки объекта защиты, которые могут облегчить проникновение противника к секретам компании. Главный результат такой работы — выявление возможных источников и каналов утечки информации.

Источники уязвимости

Уязвимости информационной системы

- Ошибки в программном обеспечении системы
- Неправильная конфигурация средств защиты
- Отсутствие установленных модулей обновления (Service packs, hotfixes, etc.)

Информационные атаки, направленные на активизацию уязвимостей системы

- Атаки, направленные на несанкционированную вставку команд в SQL-запросы
- Атаки, направленные на переполнение буфера
- Атаки, направленные на активизацию уязвимости format string

Последствия информационных атак

- Нарушение работоспособности ИС
- Искажение информации, хранящейся в системе
- Кража конфиденциальной информации

Реальное положение дел

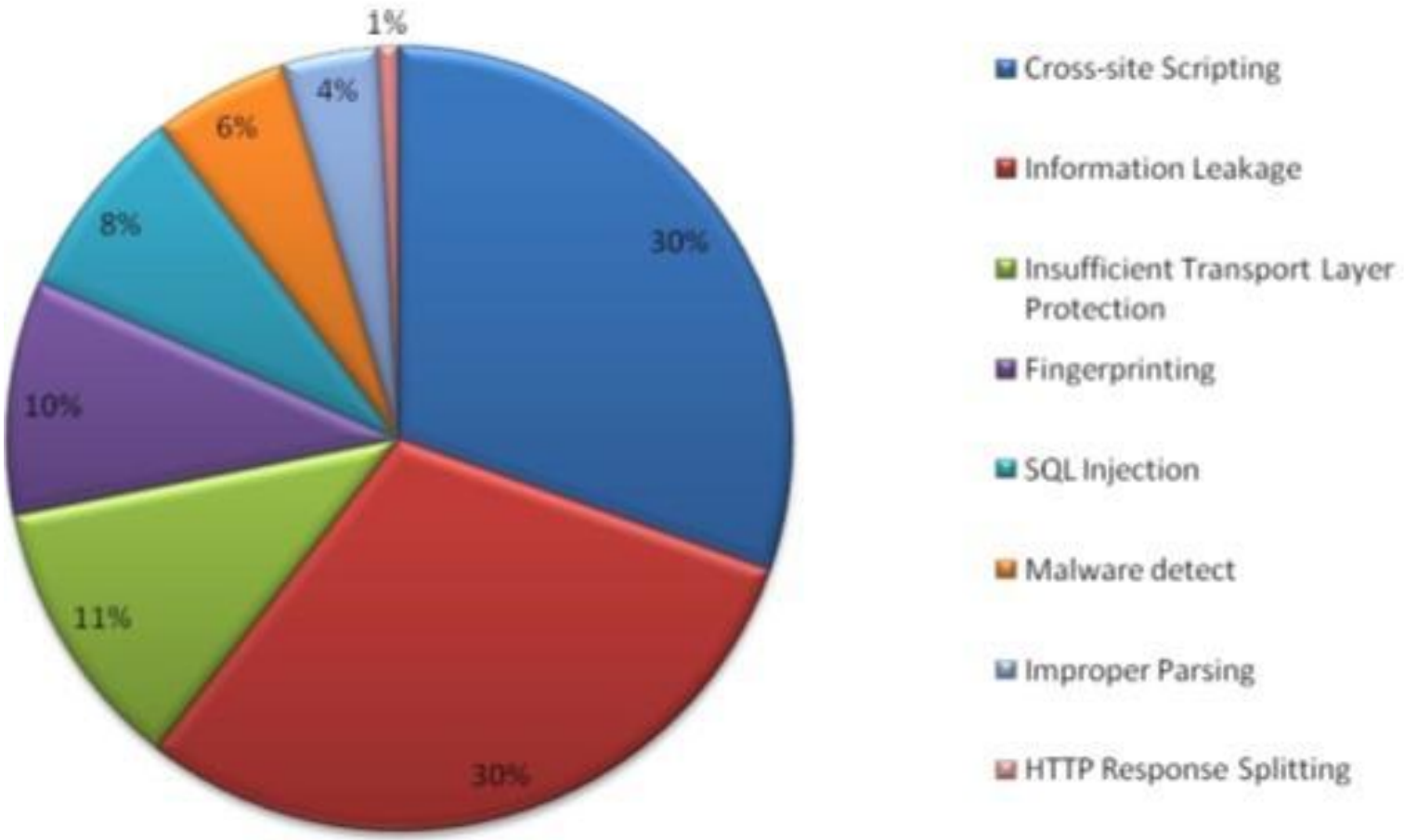


Рисунок 3. Статистика уязвимостей Web-приложений (автоматическое сканирование)

- **Аутентификация**. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).
- **Управление доступом** обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.
- **Конфиденциальность данных** обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется **конфиденциальность трафика** – это защита информации, которую можно получить, анализируя сетевые потоки данных.
- **Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
- **Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

Администрирование информационной системы в целом включает *обеспечение* актуальности политики безопасности, *взаимодействие* с другими административными службами, реагирование на происходящие события, *аудит* и *безопасное восстановление*.

Администрирование сервисов безопасности включает в себя *определение* защищаемых объектов, *выработку правил* подбора механизмов безопасности (при наличии альтернатив), *комбинирование механизмов* для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

1. управление криптографическими ключами (генерация и распределение);
2. управление шифрованием (установка и синхронизация криптографических параметров);
3. администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
4. управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);
5. управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
6. управление маршрутизацией (выделение доверенных путей);
7. управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ (до 2004 г.)

Федеральная служба по техническому и экспортному контролю:

В Российской Федерации информационная безопасность обеспечивается соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Гостехкомиссии России и других нормативных документов.

Наиболее общие документы были рассмотрены ранее при изучении правовых основ информационной безопасности. В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) Гостехкомиссии России, одной из задач которой является "проведение единой государственной политики в области технической защиты информации".

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская руководящие документы, играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии".

- В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:
- 1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
- 2) противодействия иностранным техническим разведкам на территории Российской Федерации;
- 3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- 4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- 5) осуществления экспортного контроля.

Сведения о государственных услугах, предоставляемых гражданам России, порядок их предоставления

Лицензирование деятельности по технической защите конфиденциальной информации

Лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации

Государственная аккредитация организаций, создавших внутрифирменные программы экспортного контроля

Экспортный контроль служит важным инструментом политики национальной безопасности.

- Основными задачами системы экспортного контроля в России являются:
- 1) осуществление на единой нормативной и организационно-методической основе контроля за экспортом сырья, материалов, оборудования, технологий и научно-технической информации, которые имеют военное или двойное применение т.е. могут использоваться для военных и невоенных целей;
- 2) разработка списков сырья, материалов, оборудования, технологий, научно-технической информации и услуг, экспорт которых контролируется и осуществляется по лицензиям;
- 3) осуществление контроля и учета за соблюдением порядка предоставления предприятиям и организациям права экспорта стратегически важных сырьевых товаров.
- В настоящее время деятельность российской системы экспортного контроля направлена на реализацию следующих режимов контроля товаров и услуг.

- 1. Контроль за экспортом из Российской Федерации оборудования и материалов двойного применения и соответствующих технологий, используемых в ядерных целях («Лондонский клуб ядерных поставщиков»). Нормативной основой для контроля являются распоряжения Президента РФ № 827 от 11 января 1993 г., порядок контроля определен постановлением Правительства РФ № 68 от 27 января 1993 г. Гарантии импортера должны обеспечить использование предмета контракта или любых воспроизведенных его копий в заявленных целях, не связанных с любой деятельностью по созданию ядерных взрывных устройств или ядерно-топливного цикла, не находящихся под гарантиями Международного агентства по атомной энергии (МАГАТЭ), а также возможность реэкспорта только при получении письменного разрешения экспортера, согласованного в обязательном порядке с Межведомственной комиссией по экспортному контролю (КЭК РФ).

- 2. Контроль за экспортом из Российской Федерации оборудования, материалов, технологий, применяющихся при создании ракетного оружия (режим контроля за ракетными технологиями — РКРТ). Нормативной основой для контроля является распоряжение Президента РФ № 193 рп от 25 апреля 1995г.; порядок контроля определен постановлением Правительства РФ № 1178 от 19 ноября 1993 г. Гарантии импортера должны обеспечивать использование предмета контракта только в заявленных целях, не связанных с производством оружия массового уничтожения, и осуществление копирования, модернизации, реэкспорта только на основе разрешения экспортера, согласованного в обязательном порядке с КЭК РФ.

- 3. Контроль за экспортом из России возбудителей заболеваний человека, животных, растений и оборудования, которые могут быть изменены при создании бактериологического и токсичного оружия («Австралийская группа: биологическое оружие»). Нормативной основой для контроля служит распоряжение Президента РФ № 298 от 14 июня 1994 г., порядок контроля определен постановлением Правительства РФ № 1098 от 26 сентября 1994 г.
- 4. Контроль за экспортом химикатов и технологий, которые имеют мирное назначение, но могут быть использованы при создании химического оружия («Австралийская группа: химическое оружие», «Женевская конвенция»). Нормативной основой является распоряжение Президента РФ № 621 рп от 7 декабря 1994 г., порядок контроля определен постановлением Правительства РФ № 50 от 16 января 1995 г.

5. Контроль за экспортом из России товаров и технологий «двойного» назначения («Пост КОКОМ»* или Вассенаарские договоренности). Нормативной основой для контроля служит указ Президента РФ № 1268 от 26 августа 19% г., «Положение о порядке контроля за вывозом из Российской Федерации товаров и технологий двойного назначения, экспорт которых контролируется». В течение 45 лет экспорт товаров и технологий двойного назначения оставался одной из острейших международных проблем. После Второй мировой войны, чтобы воспрепятствовать вывозу стратегических товаров в коммунистические страны, был создан КОКОМ, в который входили все государства НАТО, а также Япония и Австралия.

* *КОКОМ* — Координационный комитет по контролю за экспортом.

КОКОМ был распущен весной 1995 г., а его место заняли Вассенаарские договоренности, вступившие в силу в июле 1996 г. Участниками нового механизма экспортного контроля стали, помимо государств — членов прежнего КОКОМ, страны Восточной Европы, Республика Корея и Аргентина. Договоренности учитывают интересы России, против которой еще недавно были направлены кокомовские ограничения. В частности, не устанавливаются так называемые «черные списки» стран, для которых должны существовать экспортные ограничения, на чем настаивали США. Вместе с тем при ввозе товаров и технологий двойного назначения в страны, не являющиеся участниками Вассенаарских договоренностей, их получатель берет на себя соответствующее обязательство, оформляемое импортным сертификатом.

- Как указывается в Законе РФ «О государственном регулировании внешнеторговой деятельности», экспорт из России и импорт в нее осуществляются без количественных ограничений. Последние могут вводиться в исключительных случаях Правительством РФ.
- Существующие ограничения можно разделить на следующие категории: ограничение курса экспортеров, которым разрешается вывозить данный товар; ограничение количества товара, которое разрешено вывозить из России (квотирование); соблюдение специальных условий, исключающих возможность нанесения ущерба национальным интересам в результате экспорта.
- Количественные ограничения экспорта вводятся с целью предотвращения опустошения внутреннего рынка в условиях, когда реализация товара за рубежом выгоднее, чем внутри страны, а также чтобы исключить избыточное предложение данного товара на мировых рынках, которое может резко снизить цены и улучшить условия торговли.

Количество экспортеров, которым разрешается работать с определенным видом товара, до сих пор ограничивалось в двух случаях. Экспорт так называемых стратегически важных сырьевых товаров (в этот список входили нефть, нефтепродукты, природный газ, электроэнергия, древесина хвойных пород и др.) мог осуществляться только предприятиями и организациями, зарегистрированными для данной цели Министерством внешних экономических связей (спецэкспортеры). Согласно постановлению Правительства РФ № 758 от 1 июля 1994 г. такие товары могут вывозиться только по зарегистрированным контрактам. Однако указ Президента РФ № 245 от 6 марта 1995 г. упразднил институт спецэкспортеров с 25 марта 1995 г. С этой даты от предприятий, вывозящих данные товары, не требуется регистрации. Тем не менее сохраняется введенный с 1 июля 1994 г. порядок, в соответствии с которым для вывоза большинства товаров (за исключением нефти, но включая природный газ) требуется обязательная регистрация контракта. Регистрация осуществляется уполномоченным Министерства промышленности и торговли РФ в регионах по месту нахождения экспортера или по месту регистрации организации — владельца товара.

В настоящее время осталась одна категория продукции, право экспорта которой закрепляется за определенными организациями, т.е. свободная реализация ее запрещена. Внутри Российский Федерации правом ее использования обладают потребители, имеющие на это специальное разрешение. Из процесса распределения прав на экспорт такой продукции аукционы исключены.

Данный режим распространяется на продукцию военного назначения, ракетное топливо, яды и наркотические вещества, взрывчатые вещества и другие предметы по совершенствованию вооружения.

Парадигма доверия

РУКОВОДЯЩИЙ ДОКУМЕНТ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Критерии оценки безопасности информационных технологий

Введен в действие Приказом
Гостехкомиссии России
от 19.06.02 г. № 187

Цель данного документа состоит в изложении основных принципов и подходов к установлению доверия к безопасности. Данный подраздел позволит читателю понять логику построения требований доверия в ОК.

- Настоящий руководящий документ (РД) содержит систематизированный каталог
- требований к безопасности информационных технологий (ИТ), порядок и методические
- рекомендации по его использованию при задании требований, разработке, оценке и
- сертификации продуктов и систем информационных технологий по требованиям без-
- опасности информации.
- Руководящий документ разработан в развитие РД Гостехкомиссии России по
- защите информации от несанкционированного доступа и соответствует ГОСТ Р
- ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасно-
- сти. Критерии оценки безопасности информационных технологий", далее по тексту РД
- – Общие критерии (ОК).

Разработка настоящего руководящего документа направлена на обеспечение пактического использования ГОСТ Р ИСО/МЭК 15408-2002 в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ при формировании ими требований, разработке, приобретении и применении продуктов и систем информационных технологий, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми собственником информации. Руководящий документ предназначен также для органов сертификации и испытательных лабораторий, аккредитованных в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Гостехкомиссии России), для использования при проведении оценки и сертификации безопасности ИТ.

Под безопасностью информационной технологии понимается состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

Доверие к безопасности ИТ обеспечивается, как реализацией в них необходимых функциональных возможностей, так и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, проведением независимых оценоких безопасности и контролем ее уровня при эксплуатации.

Руководящий документ состоит из трех частей.

Часть 1 РД определяет виды требований безопасности (функциональные и требования доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности) и содержит основные методические положения по оценке безопасности ИТ.

Часть 2 РД содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 РД содержит систематизированный каталог требований доверия к безопасности и оценочные уровни доверия, определяющие меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

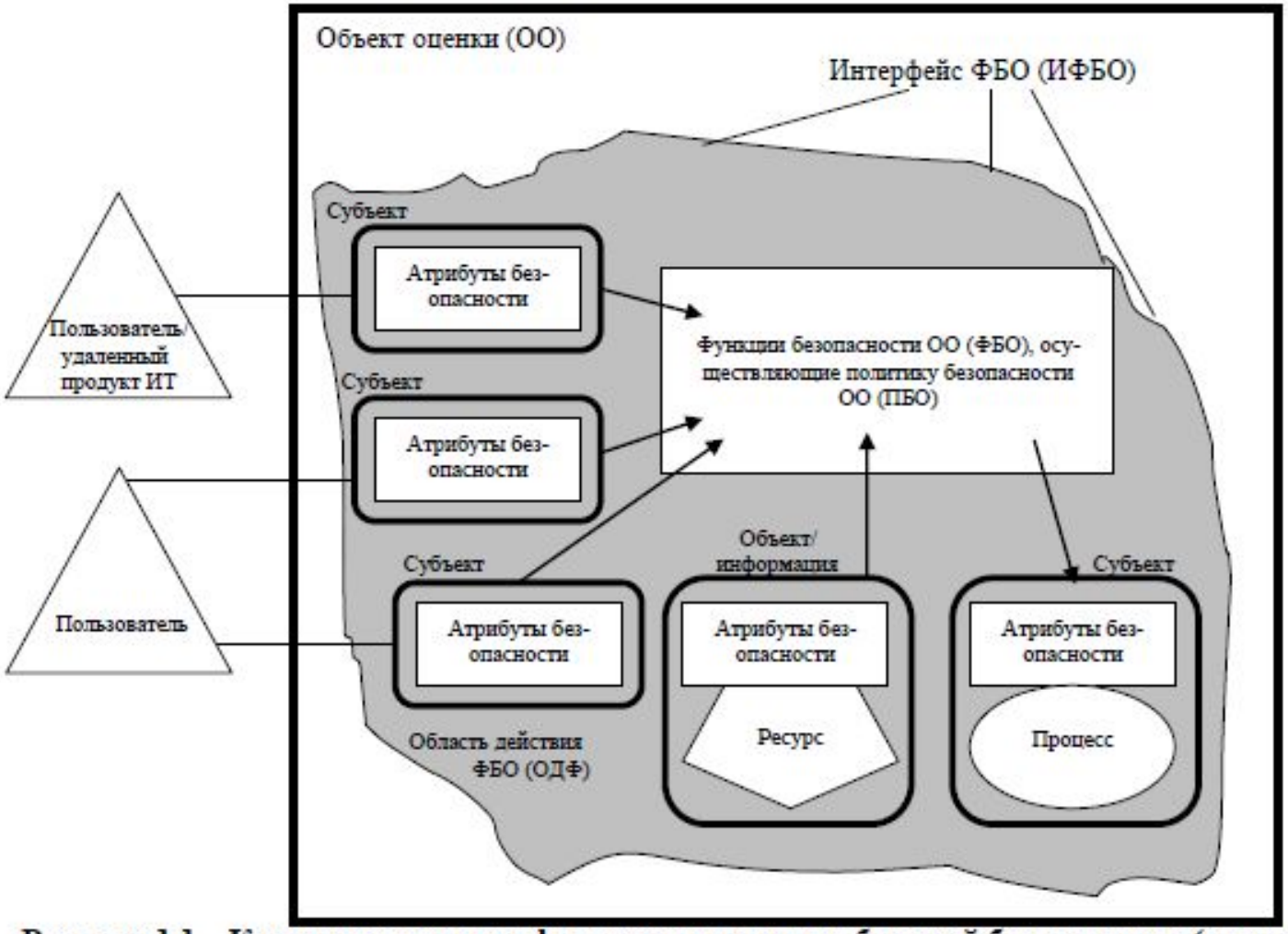


Рисунок 1.1 – Ключевые понятия функциональных требований безопасности (единый ОО)

- 6.1 ПОЛИТИКА УПРАВЛЕНИЯ ДОСТУПОМ (FDP_ACC)
- 6.2 ФУНКЦИИ УПРАВЛЕНИЯ ДОСТУПОМ (FDP_ACF)
- 6.3 АУТЕНТИФИКАЦИЯ ДАННЫХ (FDP_DAU)
- 6.4 ЭКСПОРТ ДАННЫХ ЗА ПРЕДЕЛЫ ДЕЙСТВИЯ ФБО (FDP_ETC)
- 6.5 ПОЛИТИКА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ (FDP_IFC)
- 6.6 ФУНКЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ (FDP_IFF)
- 6.7 ИМПОРТ ДАННЫХ ИЗ-ЗА ПРЕДЕЛОВ ДЕЙСТВИЯ ФБО (FDP_ITC)
- 6.8 ПЕРЕДАЧА В ПРЕДЕЛАХ ОО (FDP_ITT)
- 6.9 ЗАЩИТА ОСТАТОЧНОЙ ИНФОРМАЦИИ (FDP_RIP)
- 6.10 ОТКАТ (FDP_ROL)
- 6.11 ЦЕЛОСТНОСТЬ ХРАНИМЫХ ДАННЫХ (FDP_SDI)
- 6.12 ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЯ ПРИ ПЕРЕДАЧЕ МЕЖДУ ФБО (FDP_UCT) .
- 6.13 ЗАЩИТА ЦЕЛОСТНОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЯ ПРИ ПЕРЕДАЧЕ МЕЖДУ ФБО (FDP_UIT)

Два специфических типа данных ФБО, рассматриваемых в части 2 ОК, могут, хотя и необязательно, совпадать. Это ***аутентификационные данные и секреты.***

Аутентификационные данные используются, чтобы верифицировать заявленный идентификатор пользователя, обращающегося к ОО за услугами. Самая распространенная форма аутентификационных данных – пароль, который необходимо хранить в секрете, чтобы механизм безопасности был эффективен. Однако в секрете необходимо хранить не все формы аутентификационных данных. Биометрические опознавательные устройства (такие, как считыватели отпечатка пальца или сканеры сетчатки глаза) основываются не на предположении, что аутентификационные данные хранятся в секрете, а на том, что эти данные являются неотъемлемым свойством пользователя, которое невозможно подделать.

Термин "секрет", используемый в функциональных требованиях ОК по отношению к аутентификационным данным, применим и к данным других типов, которые необходимо хранить в тайне при осуществлении определенной ПФБ. Например, стойкость механизма доверенного канала, в котором применена криптография для сохранения конфиденциальности передаваемой через канал информации, зависит от надежности способа сохранения в секрете криптографических ключей от несанкционированного раскрытия.

Следовательно, некоторые, но не все аутентификационные данные необходимо хранить в секрете, и некоторые, но не все секреты используют как аутентификационные данные. Рисунок показывает эту взаимосвязь секретов и аутентификационных данных. На этом рисунке указаны типы данных, которые часто относят к аутентификационным данным и секретам.