**Защита информации в компьютерных сетях**

**1.1 Законодательный уровень**

Основным для обеспечения информационной безопасности является законодательный уровень. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается обществом или наказывается законом, потому что так поступать не принято. На этом уровне выделяют две группы мер:

– создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности;

– разрушение романтического ореола, существующего вокруг слова «хакер», и осознание того, что хакер – преступник, с которым вы также можете столкнуться;

– повышение общей культуры и образованности общества в области информационной безопасности, помогающее в раз-работке и распространении средств обеспечения информа-ционной безопасности.

На законодательном уровне должен работать механизм, согласующий процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но разрыв между ними и практикой не должен быть значительным, иначе этот законодательный «вакуум» будет заполнен криминалом.

**1.2 Нормативные документы и стандарты**

Все государства в вопросах информационной безопасности должны понимать друг друга, говорить «на одном языке» стандартов и нормативных технических документов. Эти документы рассматривают проблемы информационной безопасности с очень близких позиций под несколько разным ракурсом. Это оценочные стандарты, классифицирующие информационные системы и средства защиты по требованиям безопасности, и технические спецификации, предписывающие различные пути реализации средств защиты.

**1.2.1 Оценочный стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем»**

Исторически первым оценочным стандартом, получившим широкое распространение во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем», называемый по цвету обложки «Оранжевой книгой», впервые опубликованный в августе 1983 г. Этот документ описывает не безопасные, а доверенные системы, то есть системы, которым можно оказать определенную степень доверия.

«Оранжевая книга» определяет понятие безопасной системы, ко-торая «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». Поскольку безопасных систем не существует, оценивается лишь степень доверия, которую можно оказать той или иной системе.

**Доверенная система.** 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 **активному аспекту защиты –** политике безопасности и **пассивному аспекту защиты** – уровню гарантированности. Политика безопасности – правила и нормы поведения, определяющие, как организация обрабатывает и защищает информацию. Чем выше степень доверия системе, тем строже и многообразнее политика безопасности. Политика безопасности – активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации информационной системы. Доверие безопасности основано на анализе результатов тестирования и проверки общего замысла и реализации системы. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это – пассивный аспект защиты.

**Механизмы безопасности**. Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы:

– произвольное управление доступом;

– безопасность повторного использования объектов;

– метки безопасности;

– принудительное управление доступом.

**Классы безопасности**. «Критерии» Министерства обороны США допускают ранжирование информационных систем по степени доверия безопасности. Определяется четыре уровня доверия – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жёсткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности – C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, её политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям.

В своё время публикация «Оранжевой книги» стала эпохальным событием в области безопасности информации. Появился обще-признанный понятийный базис, без которого обсуждение проблем информационной безопасности было бы затруднительным. Конечно, на момент публикации (1983 г.) компьютерные сети были ещё в зачаточном состоянии и поэтому в «Оранжевой книге» вопросы безопасности распределённых систем не рассматриваются.

**1.2.2 Информационная безопасность распределённых систем. Рекомендации Международного союза телекоммуникаций (ITU) X.800**

Документ Х.800 является технической спецификацией, предписывающей различные способы реализации информационной безопасности и защиты компьютерных сетей. Документ описывает следующие **сетевые функции безопасности, сервисы безопасности:**

– аутентификация – проверка подлинности партнёров по об-щению;

– управление доступом – обеспечение защиты от несанкцио-нированного использования ресурсов, доступных по сети;

– конфиденциальность данных – обеспечение защиты от не-санкционированного получения информации;

– целостность данных – защита данных от несанкционирован-ного изменения;

– неотказуемость – подтверждение подлинности данных и не-возможность отказа от совершённых действий.

Документ Х.800 широко использует стандарт семиуровневой мо-дели открытых систем OSI, на которых реализуются перечислен-ные выше сервисы безопасности. Поддержку всех сервисов можно реализовать на уровне приложений.

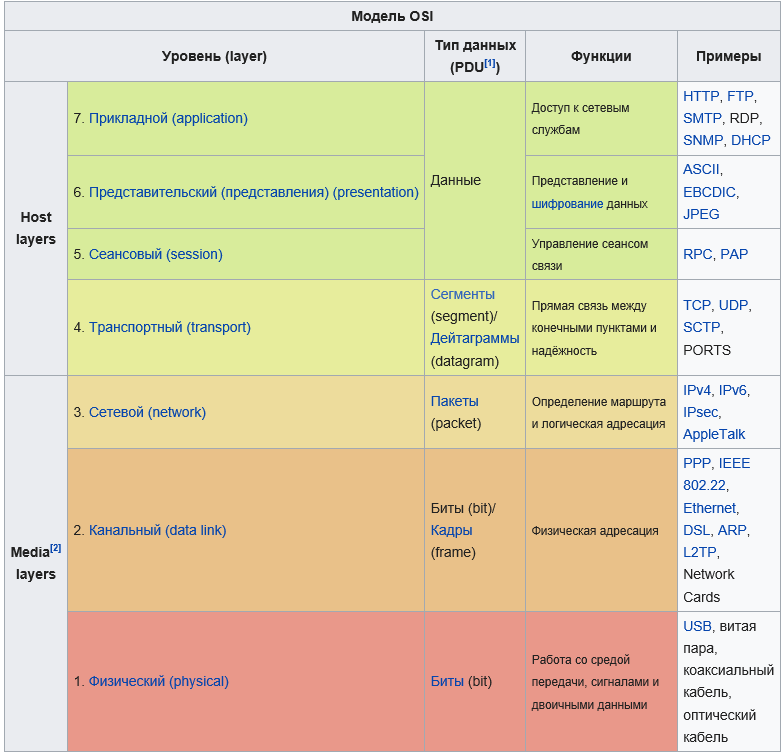


Рисунок 0. Семиуровневая модель OSI

**1.2.3 Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»**

«Критерии оценки безопасности информационных технологий» (изданы в 1999 г.) является оценочным стандартом. Этот между-народный стандарт – итог многолетней работы специалистов не-скольких стран, он охватывает документы национального и межнационального масштаба. По историческим причинам данный стандарт часто называют «Общими критериями».

«Общие критерии» (ОК) на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от «Оранжевой книги» ОК не содер-жат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существую-щих для конкретной организации и/или конкретной информационной системы.

Как и «Оранжевая книга», «Общие критерии» содержат два основных вида требований безопасности:

– функциональные, соответствующие **активному аспекту защиты**, предъявляемые к функциям безопасности и реали-зующим их механизмам;

– требования доверия, соответствующие **пассивному аспекту защиты**, предъявляемые к технологии, процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки – аппаратно-программного продукта или информационной системы. Безопасность в «Общих критериях» рассматривается в привязке к жизненному циклу объекта оценки. Выделяются следующие **этапы:**

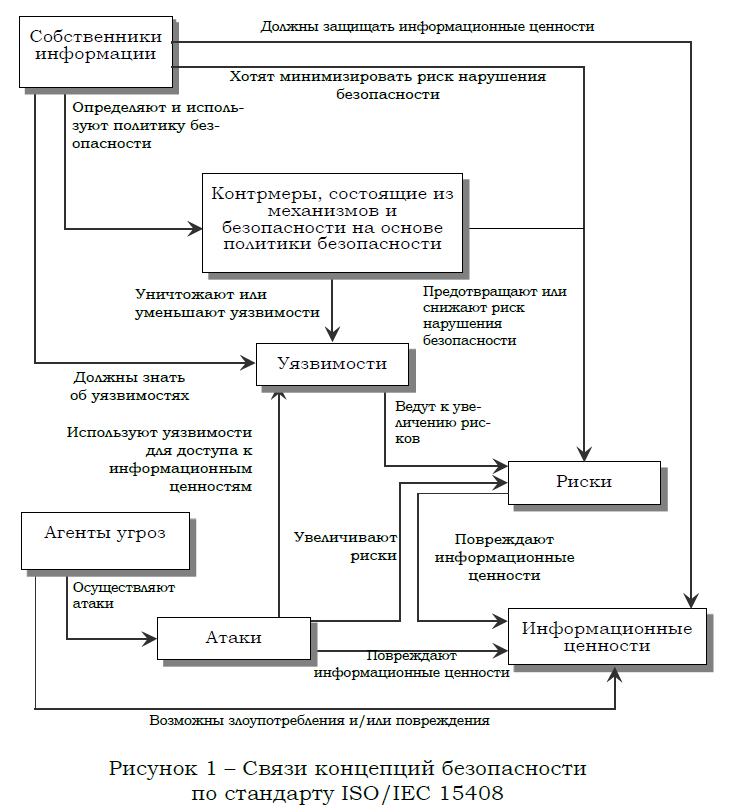
– определение назначения, условий применения, целей и тре-бований безопасности;

– проектирование и разработка;

– испытания, оценка и сертификация;

– внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами (рисунок 1).



**Собственник** определяет множество **информационных ценностей**, которые должны быть защищены от различного рода атак. Атаки осуществляются противниками или оппонентами, использующими различные уязвимости в защищаемых ценностях. Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря конфиденциальности), их неавторизованная модификация (потеря целостности) или неавторизованная потеря доступа к этим ценностям (потеря доступности). Собственники информационных ценностей анализируют уязвимости защищаемых ресурсов и возможные атаки, которые могут иметь место в конкретном окружении. В результате такого анализа определяются риски для данного набора информационных ценностей. Этот анализ определяет выбор контрмер, который задается политикой безопасности и обеспечивается с помощью механизмов и сервисов безопасности. Следует учитывать, что отдельные уязвимости могут сохраниться и после применения механизмов и сервисов безопасности. Политика безопасности определяет согласованную совокупность механизмов и сервисов безопасности, адекватную защищаемым ценностям и окружению, в котором они используются.

В «Общих критериях» используются следующие определения.

**Уязвимость** – слабое место в системе, с использованием которого может быть осуществлена атака.

**Риск** – вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости. В конечном счете каждая организация должна принять решение о допустимом для нее уровне риска. Это решение должно найти отражение в политике безопасности, принятой в организации.

**Политика безопасности** – правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления сервисов безопасности.

**Атака** – любое действие, нарушающее безопасность информаци-онной системы. Более формально можно сказать, что атака – это действие или последовательность связанных между собой дей-ствий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности.

**Механизм безопасности** – программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.

**Сервис безопасности** – сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление атаки. Сервис использует один или более механизмов безопасности.

**1.3 Административный уровень**

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации. Главная цель мер административного уровня [3] – сформировать программу работ в области информационной безопасности и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информацион-ной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы.

**1.3.1 Политика безопасности**

Политика безопасности – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации. С практической точки зрения политика безопасности рассматривается на трёх уровнях. К **верхнему уровню** относятся решения, затрагивающие организацию в целом. Они носят общий характер и исходят от руководства организации. Примерный список подобных решений может включать в себя следующие **элементы:**

– решение сформировать комплексную программу обеспечения информационной безопасности, назначение ответственных за её осуществление;

– формулировка целей организации в области информационной безопасности, определение общих направлений в достижении этих целей;

– обеспечение базы для соблюдения законов и правил;

– формулировка административных решений по вопросам ре-ализации программы безопасности.

Для **политики верхнего уровня** цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На **верхний уровень** выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности. Политика верхнего уровня должна чётко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

**В политике определяются** обязанности должностных лиц по выработке программы безопасности и претворению её в жизнь. Политика верхнего уровня имеет дело с **тремя аспектами** законопослушности и исполнительской дисциплины. **Во-первых,** организация должна соблюдать существующие законы. **Во-вторых**, следует контролировать действия лиц, ответственных за выработку программы безопасности. **Наконец**, необходимо обеспечить определённую степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

На верхний уровень следует выносить минимум вопросов. Это целесообразно в случае экономии средств или когда иначе поступить просто невозможно.

**Британский стандарт BS 7799:1995** рекомендует включать в документ, характеризующий политику безопасности организации, следующие **разделы:**

– вводный, подтверждающий озабоченность высшего руко-водства проблемами информационной безопасности;

– организационный, содержащий описание подразделений, комиссий, групп, отвечающих за работы в области инфор-мационной безопасности;

– классификационный, описывающий имеющиеся в организа-ции материальные и информационные ресурсы и необходимый уровень их защиты;

– штатный, характеризующий меры безопасности, применяе-мые к персоналу (описание должностей с точки зрения ин-формационной безопасности, организация обучения и пере-подготовки персонала, порядок реагирования на нарушения режима безопасности);

– раздел, освещающий вопросы физической защиты;

– управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;

– раздел, описывающий правила разграничения доступа к производственной информации;

– раздел, характеризующий порядок разработки и сопровождения систем;

– раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;

– юридический раздел, подтверждающий соответствие поли-тики безопасности действующему законодательству.

К **среднему уровню** можно отнести вопросы, касающиеся от-дельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов – отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения.

Политика среднего уровня должна для каждого аспекта освещать следующие **темы.**

**Описание аспекта**. Например, если рассмотреть применение пользователями неофициального программного обеспечения, по-следнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

**Область применения**. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на компьютеры своих рабочих мест?

**Позиция организации по данному аспекту**. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности, в разных организациях может сильно отличаться.

**Роли и обязанности**. В документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

**Законопослушность**. Политика должна содержать общее описание запрещенных действий и наказаний за них.

**Точки контакта**. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определённое должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности **нижнего уровня** относится к конкретным информационным сервисам. Она включает в себя два аспекта – цели и правила их достижения, поэтому её порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в **политике безопасности нижнего уровня:**

1 Кто имеет право доступа к объектам, поддерживаемым сервисом?

2 При каких условиях можно читать и модифицировать дан-ные?

3 Как организован удалённый доступ к сервису?

При формулировке целей политики нижнего уровня можно исхо-дить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Её цели должны быть более конкретными. Например, если речь идёт о системе расчёта заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жёсткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

**1.3.2 Программа безопасности**

После того, как сформулирована политика безопасности, можно приступать к составлению программы её реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, её нужно структурировать по уровням, обычно в соответствии со структу-рой организации. В простейшем и самом распространенном слу-чае достаточно двух уровней – верхнего, или центрального, кото-рый охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

**Программу верхнего уровня** возглавляет лицо, отвечающее за информационную безопасность организации. Главные цели про-граммы следующие:

– управление рисками (оценка рисков, выбор эффективных средств защиты);

– координация деятельности в области информационной без-опасности, пополнение и распределение ресурсов;

– стратегическое планирование;

– контроль деятельности в области информационной безопас-ности.

**В рамках** **программы верхнего уровня** принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, поэтому необходимо иметь чёткую политику контроля и внедрения новых средств.

Контроль деятельности в области безопасности имеет двусторон-нюю направленность. **Во-первых**, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. **Во-вторых**, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать меры защиты с учётом изменения обстановки. Следует подчеркнуть, что программа верхнего уровня должна занимать строго определённое место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определённый штат и бюджет.

**Цель программы нижнего уровня** – обеспечить надёжную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест. Обычно за программу нижнего уровня отвечают администраторы сервисов.

**1.3.3 Синхронизация программы безопасности с жизненным циклом систем**

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие **этапы.**

**Инициация**. На данном этапе выявляется необходимость в при-обретении нового сервиса, документируется его предполагаемое назначение.

**Закупка**. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

**Установка**. Сервис устанавливается, конфигурируется, тестиру-ется и вводится в эксплуатацию.

**Эксплуатация**. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

**Выведение из эксплуатации**. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие **вопросы:**

1 Какого рода информация предназначается для обслуживания новым сервисом?

2 Каковы возможные последствия нарушения конфиденци-альности, целостности и доступности этой информации?

3 Каковы угрозы, по отношению к которым сервис и инфор-мация будут наиболее уязвимы?

4 Есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?

5 Каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?

6 Каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

**Этап закупки** – один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Установка является очень ответственным делом. **Во-первых**, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоёмким и ответственным делом.

**Во-вторых**, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей. После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации – самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось, на самом же деле от былой безопасности не осталось и следа.

Для борьбы с **эффектом медленных изменений** приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

**При выведении данных из эксплуатации** их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

**1.4 Процедурный уровень. Основные классы мер процедурного уровня**

На процедурном уровне рассматриваются меры безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания [9].

На процедурном уровне можно выделить следующие классы мер:

– управление персоналом;

– физическая защита;

– поддержание работоспособности;

– реагирование на нарушения режима безопасности;

– планирование восстановительных работ.

**1.4.1 Управление персоналом**

Управление персоналом начинается с приёма нового сотрудника на работу и даже раньше – с составления должностной инструк-ции. Уже на данном этапе желательно подключить к работе спе-циалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

– разделение обязанностей;

– минимизация привилегий.

**Принцип разделения обязанностей** предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоём, что снижает вероятность ошибок и злоупотреблений.

**Принцип минимизации привилегий** предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить её критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять её. В то же время неразумно и совсем отказываться от предварительной проверки.

Когда кандидат определён, он, вероятно, должен пройти обучение; по крайней мере его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до создания его учётной записи в системе с входным именем, паролем и привилегиями.

С момента заведения учётной записи начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности. Всё это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

**Ликвидация учётной записи пользователя**, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно. Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять всё его компьютерное «хозяйство» и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту. В соответствии с принципом минимизации привилегий им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения «внешние» сотрудники будут администрировать «местных», а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнёров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удалённом режиме. Вообще говоря, это создаёт в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удалённого доступа или обучением собственных сотрудников.

**Проблема обучения** – одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Не зная мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

**1.4.2 Физическая защита**

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных. Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как «непрерывность защиты в пространстве и времени».

Мы кратко рассмотрим следующие направления физической за-щиты:

– физическое управление доступом;

– противопожарные меры;

– защита поддерживающей инфраструктуры;

– защита от перехвата данных;

– защита мобильных систем.

Меры **физического управления доступом** позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может всё здание организации, а также отдельные помещения. Нужно сделать так, чтобы посетители по возможности не имели непосредственного доступа к компьютерам или в крайнем случае позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят «без опознавательных знаков», злоумышленнику достаточно снять карточку, чтобы его считали «своим». Очевидно, соответ-ствующие карточки нужно выдавать всем.

**Средства физического управления доступом** известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального средства целесообразно провести анализ рисков.

Необходимо установка противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, что защитные меры могут создавать новые слабые места. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам нарушает рабочий режим, то ввиду повышенной пожароопасности подобная мера защиты может только навредить.

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но могут нанести огромный ущерб. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок. Необходимо повсеместно использовать криптографию, стараться максимально расширить контролируемую территорию, разместившись поодаль, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероятно, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. Необходимо шифровать данные на жёстких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией, характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий. В то же время во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но всё же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

**1.4.3 Поддержание работоспособности**

Существует ряд рутинных мероприятий, направленных на под-держание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки систем-ных администраторов и пользователей грозят повреждением ап-паратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе – ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

– поддержка пользователей;

– поддержка программного обеспечения;

– конфигурационное управление;

– резервное копирование;

– управление носителями;

– документирование;

– регламентные работы.

**Поддержка пользователей** подразумевает прежде всего консультирование и оказание помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный «справочный стол», но чаще от пользователей «отбивается» системный администратор. Очень важно в потоке вопросов уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

**Поддержка программного обеспечения** – одно из важнейших средств обеспечения целостности информации. Прежде всего необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что «самодеятельность» пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придётся системному администратору.

**Второй аспект** поддержки программного обеспечения – контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

**Резервное копирование** необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами. Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов.

**Документирование** – неотъемлемая часть информационной без-опасности. В виде документов оформляется почти всё – от политики безопасности до журнала учёта носителей. К хранению одних документов применимы требования обеспечения конфиденциальности, других, таких как план восстановления после аварий, – требования целостности и доступности.

**Регламентные работы** – очень серьёзная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно контролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

**1.4.4 Реагирование на нарушения режима безопасности**

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

**Реакция на нарушения режима безопасности** преследует три главные цели:

– локализация инцидента и уменьшение наносимого вреда;

– выявление нарушителя;

– предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки, который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить и что делать до приезда пожарной команды.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, на наш взгляд, в первую очередь следует заботиться о минимизации ущерба.

Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

**1.4.5 Планирование восстановительных работ**

Ни одна организация не застрахована от серьёзных аварий, вы-званных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объёме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на **предупреждение, обнаружение или ликвидацию** последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

**Процесс планирования восстановительных работ** можно разделить на следующие этапы:

– выявление критически важных функций организации, уста-новление приоритетов;

– идентификация ресурсов, необходимых для выполнения критически важных функций;

– определение перечня возможных аварий;

– разработка стратегии восстановительных работ;

– подготовка к реализации выбранной стратегии;

– проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчёт в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет своё лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

– персонал;

– информационная инфраструктура;

– физическая инфраструктура.

Составляя списки ответственных специалистов, следует учиты-вать, что некоторые из них могут непосредственно пострадать от аварии (например от пожара), кто-то может находиться в состоянии стресса, часть сотрудников может лишиться возможности попасть на работу (например в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдёт с критичными ресурсами? Например, смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

**Стратегия восстановительных работ** должна базироваться на наличных ресурсах и быть не слишком накладной для организа-ции. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение. Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выра-ботке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий – те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копиро-вания, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах). Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях.

**1.5 Программно-технический уровень**

**1.5.1 Основные понятия программно-технического уровня информационной безопасности**

Программно-технические меры, то есть меры, направленные на контроль оборудования, программ и данных, образуют последний и один из самых важных рубежей информационной безопасности. Как показывает статистика, ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные «враги» – некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

**С одной стороны**, быстрое развитие информационных технологий предоставляет «обороняющимся» новые возможности, но, с другой стороны, затрудняет обеспечение надёжной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

– повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет взламывать ранее казавшиеся неприступными барьеры;

– развитие сетей и сетевых технологий, увеличение числа свя-зей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;

– появление новых информационных сервисов ведёт и к обра-зованию новых уязвимых мест;

– конкуренция среди производителей программного обеспече-ния заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;

– навязываемая потребителям парадигма постоянного нара-щивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надёжных, апробированных конфигураций.

Для программно-технического уровня основным является понятие **сервиса безопасности**, в который входят:

– идентификация и аутентификация;

– управление доступом;

– протоколирование и аудит;

– шифрование;

– контроль целостности;

– экранирование;

– анализ защищенности;

– обеспечение отказоустойчивости;

– обеспечение безопасного восстановления;

– туннелирование;

– управление.

**1.5.2 Особенности современных информационных систем, существенные с точки зрения безопасности**

Информационная система современной организации является весьма сложным образованием, которое пользуется многочисленными внешними сервисами и в свою очередь предоставляет собственные сервисы вовне.

Следует учитывать ещё по крайней мере два момента. **Во-первых**, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения системы управления базами данных и с точки зрения почтового сервера – вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует анализировать защищенность сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному.

**Во-вторых**, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников.

В силу изложенных причин далее будут рассматриваться распределённые, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

**1.5.3 Архитектурная безопасность**

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

С практической точки зрения наиболее важными являются следующие **принципы архитектурной безопасности:**

– непрерывность защиты в пространстве и времени, невоз-можность миновать защитные средства;

– следование признанным стандартам, использование апроби-рованных решений;

– иерархическая организация ИС с небольшим числом сущно-стей на каждом уровне;

– усиление самого слабого звена;

– невозможность перехода в небезопасное состояние;

– минимизация привилегий;

– разделение обязанностей;

– эшелонированность обороны;

– разнообразие защитных средств;

– простота и управляемость информационной системы.

Кратко смысл перечисленных принципов заключается в следую-щем.

Если **непрерывность** нарушена, тогда у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает.

Следование **признанным стандартам** и использование апроби-рованных решений повышает надежность ИС и уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

**Иерархическая организация** ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет неуправляемой и, следовательно, обеспечить ее безопасность будет невозможно.

Надёжность любой обороны определяется самым **слабым звеном**. Злоумышленник не будет бороться против силы, он предпочтёт легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности **перехода в небезопасное состояние** означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

Применительно к программно-техническому уровню принцип **минимизации привилегий** предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Этот принцип позволяет уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип **разделения обязанностей** предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. В частности, соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип **эшелонированности обороны** предписывает не пола-гаться на один защитный рубеж, каким бы надёжным он ни ка-зался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и как последний рубеж – протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а благодаря наличию такого рубежа, как протоколирование и аудит, его действия не останутся незамеченными.

Принцип **разнообразия защитных** средств предполагает созда-ние различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными и по возможности несовместимыми между собой навыками.

Очень важен **принцип простоты и управляемости** информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование.