Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности

В деле обеспечения информационной безопасности успех может принести только *комплексный подход*. Для защиты интересов *субъектов информационных отношений* необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их ***мерами ограничительной направленности***);
- ***направляющие и координирующие меры***, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех *субъектов информационных отношений*, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

ЗАКОН РЕСПУБЛИКИ КАЗАХСТАН

Об информатизации *(с изменениями и дополнениями по состоянию на 02.01.2021 г.)*

РАЗДЕЛ 1. ОСНОВЫ РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные понятия, используемые в настоящем Законе

29-1) мониторинг событий информационной безопасности - постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий информационной безопасности;

30) событие информационной безопасности - состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации;

Статья дополнена подпунктом 30-1 в соответствии с Законом РК от 28.12.17 г. № 128-VI; изложен в редакции Закона РК от 25.06.20 г. № 347-VI (см. стар. ред.)

30-1) система мониторинга обеспечения информационной безопасности - организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования информационно-коммуникационных технологий;

Статья дополнена подпунктом 30-2 в соответствии с Законом РК от 28.12.17 г. № 128-VI; изложен в редакции Закона РК от 25.06.20 г. № 347-VI (см. стар. ред.)

31-1) отраслевой центр информационной безопасности - юридическое лицо или структурное подразделение уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций, осуществляющее деятельность по координации обеспечения информационной безопасности финансового рынка и финансовых организаций, филиалов банков - нерезидентов Республики Казахстан, филиалов страховых (перестраховочных) организаций - нерезидентов Республики Казахстан, филиалов страховых брокеров - нерезидентов Республики Казахстан;

32) средство защиты информации - программное обеспечение, технические и иные средства, предназначенные и используемые для обеспечения защиты информации;

Статья дополнена подпунктом 32-1 в соответствии с Законом РК от 02.01.21 г. № 399-VI

32-1) аппаратно-программный комплекс - совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа;

Подпункт 33 изложен в редакции Закона РК от 02.01.21 г. № 399-VI (см. стар. ред.)

Глава 2. ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ В СФЕРЕ ИНФОРМАТИЗАЦИИ

Статья 5. Основные задачи государственного управления в сфере информатизации

Основными задачами государственного управления в сфере информатизации являются:

9) формирование, развитие и защита государственных электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечение их взаимодействия в едином информационном пространстве;

10) мониторинг обеспечения информационной безопасности государственных органов, физических и юридических лиц;

11) предупреждение и оперативное реагирование на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения;

12) создание условий для привлечения инвестиций в отрасль информационно-коммуникационных технологий на системной основе;

Статья 7-2. Оперативный центр информационной безопасности

1. Оперативный центр информационной безопасности:

1) осуществляет деятельность по обнаружению, оценке, прогнозированию, локализации, нейтрализации и профилактике угроз информационной безопасности информационно-коммуникационной инфраструктуры, объектов информатизации, подключенных к оперативному центру информационной безопасности;

2) принимает меры по минимизации угроз информационной безопасности, незамедлительно информирует владельца информационно-коммуникационной инфраструктуры, а также Национальный координационный центр информационной безопасности о факте инцидента информационной безопасности;

Подпункт 3 изложен в редакции Закона РК от 18.03.19 г. № 237-VI (введены в действие с 30 марта 2019 г.) (см. стар. ред.)

3) осуществляет мониторинг обеспечения информационной безопасности критически важных объектов информационно-коммуникационной инфраструктуры, объектов информатизации, не относящихся к объектам информатизации «электронного правительства»;

4) осуществляет обмен информацией, необходимой для обеспечения информационной безопасности объектов информатизации, подключенных к оперативному центру информационной безопасности, с Национальным координационным центром информационной безопасности и другими оперативными центрами информационной безопасности;

5) осуществляет сбор, консолидацию, анализ и хранение сведений о событиях и инцидентах информационной безопасности;

6) предоставляет владельцам критически важных объектов информационно-коммуникационной инфраструктуры информацию, необходимую для обеспечения информационной безопасности объектов информационно-коммуникационной инфраструктуры, в том числе информацию об угрозах безопасности, уязвимости программного обеспечения, оборудования и технологий, способах реализации угроз информационной безопасности, предпосылках возникновения инцидентов информационной безопасности, а также методах их предупреждения и ликвидации последствий;

7) обеспечивает сохранность сведений ограниченного распространения, ставших известными оперативному центру информационной безопасности в рамках осуществления его деятельности;

Статья 7-4. Национальный координационный центр информационной безопасности

1. Национальный координационный центр информационной безопасности:

1) содействует собственникам, владельцам и пользователям объектов информатизации в вопросах безопасного использования информационно-коммуникационных технологий;

Подпункт 2 изложен в редакции Закона РК от 03.07.19 г. № 262-VI (введено в действие с 1 января 2020 г.) (см. стар. ред.)

2) обеспечивает взаимодействие оперативных и отраслевого центров информационной безопасности финансового рынка и финансовых организаций;

3) осуществляет сбор, анализ и обобщение информации оперативных центров информационной безопасности об инцидентах информационной безопасности на объектах информационно-коммуникационной инфраструктуры «электронного правительства» и других критически важных объектах информационно-коммуникационной инфраструктуры;

Подпункт 4 изложен в редакции Закона РК от 25.06.20 г. № 347-VI (см. стар. ред.)

4) обеспечивает функционирование объектов информационно-коммуникационной инфраструктуры Национального координационного центра информационной безопасности;

Статья 14-1. Национальный институт развития в сфере обеспечения информационной безопасности

Национальный институт развития в сфере обеспечения информационной безопасности:

1) участвует в реализации государственной политики в сфере обеспечения информационной безопасности;

2) разрабатывает документы по стандартизации в сфере обеспечения информационной безопасности;

3) осуществляет научно-техническую деятельность в сфере обеспечения информационной безопасности;

4) проводит научно-техническую экспертизу проектов в сфере обеспечения информационной безопасности;

5) осуществляет подготовку, переподготовку и повышение квалификации в сфере информационной безопасности.

Глава 9. ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Статья 53. Цели защиты объектов информатизации

1. Защитой объектов информатизации является реализация комплекса правовых, организационных и технических мероприятий, направленных на сохранность объектов информатизации, предотвращение неправомерного и (или) непреднамеренного доступа и (или) воздействия на них.

2. Защита объектов информатизации осуществляется в соответствии с законодательством Республики Казахстан и действующими на территории Республики Казахстан стандартами в целях:

1) обеспечения целостности и сохранности электронных информационных ресурсов;

2) обеспечения режима конфиденциальности электронных информационных ресурсов ограниченного доступа;

3) реализации права субъектов информатизации на доступ к электронным информационным ресурсам;

4) недопущения несанкционированного и (или) непреднамеренного доступа, утечки и иных действий в отношении электронных информационных ресурсов, а также несанкционированного и (или) непреднамеренного воздействия на объекты информационно-коммуникационной инфраструктуры;

5) недопущения нарушений функционирования объектов информационно-коммуникационной инфраструктуры и критически важных объектов информационно-коммуникационной инфраструктуры;

Пункт дополнен подпунктами 6, 7 в соответствии с Законом РК от 25.06.20 г. № 347-VI

6) недопущения несанкционированного и (или) непреднамеренного доступа к служебной информации об абонентах сетей телекоммуникаций и сообщениям телекоммуникаций;

7) недопущения несанкционированного и (или) непреднамеренного блокирования работы абонентских устройств сетей телекоммуникаций.

3. Иными несанкционированными и (или) непреднамеренными действиями в отношении объектов информатизации являются:

1) блокирование электронных информационных ресурсов и (или) объектов информационно-коммуникационной инфраструктуры, то есть совершение действий, приводящих к ограничению или закрытию доступа к электронным информационным ресурсам и (или) объектам информационно-коммуникационной инфраструктуры;

2) несанкционированная и (или) непреднамеренная модификация объектов информатизации;

3) несанкционированное и (или) непреднамеренное копирование электронного информационного ресурса;

4) несанкционированное и (или) непреднамеренное уничтожение, утрата электронных информационных ресурсов;

5) использование программного обеспечения без разрешения правообладателя;

6) нарушение работы информационных систем и (или) программного обеспечения либо нарушение функционирования сети телекоммуникаций;

Пункт дополнен подпунктами 7, 8 в соответствии с Законом РК от 25.06.20 г. № 347-VI

7) несанкционированный и (или) непреднамеренный доступ к служебной информации об абонентах сетей телекоммуникаций и сообщениям телекоммуникаций;

8) несанкционированное и (или) непреднамеренное блокирование работы абонентских устройств сетей телекоммуникаций.

4. Защита информационных систем осуществляется согласно классу, присвоенному в соответствии с классификатором.

Статья 54. Организация защиты объектов информатизации

1. Защита объектов информатизации осуществляется:

1) в отношении электронных информационных ресурсов - их собственниками, владельцами и пользователями;

2) в отношении объектов информационно-коммуникационной инфраструктуры и критически важных объектов информационно-коммуникационной инфраструктуры - их собственниками или владельцами.

2. Собственники или владельцы объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры обязаны принимать меры, обеспечивающие:

1) предотвращение несанкционированного доступа;

2) своевременное обнаружение фактов несанкционированного доступа, если такой несанкционированный доступ не удалось предотвратить;

3) минимизацию неблагоприятных последствий нарушения порядка доступа;

4) недопущение несанкционированного воздействия на средства обработки и передачи электронных информационных ресурсов;

5) оперативное восстановление электронных информационных ресурсов, модифицированных либо уничтоженных вследствие несанкционированного доступа к ним;

В подпункт 6 внесены изменения в соответствии с Законом РК от 18.03.19 г. № 237-VI (введены в действие с 30 марта 2019 г.) (см. стар. ред.)

6) незамедлительное информирование Национального координационного центра информационной безопасности о произошедшем инциденте информационной безопасности, за исключением собственников и (или) владельцев электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты;

В подпункт 7 внесены изменения в соответствии с Законом РК от 18.03.19 г. № 237-VI (введены в действие с 30 марта 2019 г.) (см. стар. ред.)

7) информационное взаимодействие с Национальным координационным центром информационной безопасности по вопросам мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства»;

В подпункт 8 внесены изменения в соответствии с Законом РК от 18.03.19 г. № 237-VI (введены в действие с 30 марта 2019 г.) (см. стар. ред.)

8) предоставление доступа Национальному координационному центру информационной безопасности к объектам информатизации «электронного правительства» и оперативным центрам информационной безопасности к критически важным объектам информационно-коммуникационной инфраструктуры для проведения организационно-технических мероприятий, направленных на реализацию мониторинга обеспечения информационной безопасности в соответствии с правилами проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 55. Меры защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры

1. К правовым мерам защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры относятся:

1) требования законодательства Республики Казахстан и действующие на территории Республики Казахстан стандарты в сфере информатизации;

2) ответственность за нарушение законодательства Республики Казахстан об информатизации;

3) соглашения, заключаемые собственником или владельцем электронных информационных ресурсов, информационных систем, информационно-коммуникационной инфраструктуры, в которых устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение.

2. К организационным мерам защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры относятся установление и обеспечение режима допуска на территории (в здания, помещения), где может быть осуществлен доступ к информации, электронным информационным ресурсам, информационным системам (электронным носителям информации), а также ограничение доступа к электронным информационным ресурсам, информационным системам и информационно-коммуникационной инфраструктуре.

3. К техническим (программно-техническим) мерам защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры относятся:

1) использование средств защиты информации, а в отношении сведений, составляющих государственные секреты, - исключительно с применением средств защиты сведений, составляющих государственные секреты, разработанных, изготовленных и (или) принятых в эксплуатацию в соответствии с законодательством Республики Казахстан;

2) использование систем контроля доступа и регистрации фактов доступа к электронным информационным ресурсам, информационным системам и информационно-коммуникационной инфраструктуре;

Пункт 3 дополнен подпунктом 3 в соответствии с Законом РК от 28.12.17 г. № 128-VI

3) разработка задания по безопасности на основе утвержденных профилей защиты для определения мер защиты собственниками или владельцами объектов информатизации.

4. Использование технических (программно-технических) мер защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры не должно причинять вред или создавать угрозу причинения вреда жизни, здоровью и имуществу физических лиц, а также имуществу юридических лиц и государственному имуществу.

Статья 56. Защита электронных информационных ресурсов, содержащих персональные данные

Собственники и владельцы информационных систем, получившие электронные информационные ресурсы, содержащие персональные данные, собственник и (или) оператор базы, содержащей персональные данные, а также третьи лица обязаны принимать меры по их защите в соответствии с настоящим Законом, законодательством Республики Казахстан о персональных данных и их защите и действующими на территории Республики Казахстан стандартами.

Данная обязанность возникает с момента получения электронных информационных ресурсов, содержащих персональные данные, или сбора персональных данных и до их уничтожения либо обезличивания.

Стандарды и сертификаты. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт

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.

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".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "*Оранжевая книга*" не затрагивает.

Степень доверия оценивается по двум основным критериям.

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.

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*.

Концепция *доверенной вычислительной базы* является центральной при оценке *степени доверия* безопасности. ***Доверенная вычислительная база*** - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь *политики безопасности*. Качество вычислительной базы определяется исключительно ее *реализацией* и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

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.

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*.

- ***Произвольное управление доступом (называемое иногда дискреционным)*** - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно *владелец объекта*) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.
- ***Безопасность повторного использования объектов*** - важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". *Безопасность повторного использования* должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Как мы указывали ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его *реализацию*. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для *реализации принудительного управления доступом* с субъектами и объектами ассоциируются *метки безопасности*. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Согласно "*Оранжевой книге*", *метки безопасности* состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

- *Принудительное (или мандатное) управление доступом* основано на сопоставлении *меток безопасности* субъекта и объекта.
- Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в *метке безопасности* объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.
- Субъект может записывать информацию в объект, если *метка безопасности* объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий).
- Описанный способ управления доступом называется *принудительным*, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы *метки безопасности* субъектов и объектов, оказываются зафиксированными и права доступа.

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.

Если фиксировать все события, объем *регистрационной информации*, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "*Оранжевая книга*" предусматривает наличие средств *выборочного протоколирования*, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в "*Оранжевой книге*" рассматривается два вида гарантированности - операционная и технологическая. *Операционная гарантированность* относится к архитектурным и реализационным аспектам системы, в то время как *технологическая* - к методам построения и *сопровождения*.

Операционная гарантированность включает в себя проверку следующих элементов:

архитектура системы;

целостность системы;

проверка *тайных каналов передачи информации* ;

доверенное администрирование;

доверенное *восстановление после сбоев*.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее *реализация* действительно реализуют избранную *политику безопасности* .

Технологическая гарантированность охватывает весь *жизненный цикл ИС*, то есть периоды *проектирования*, *реализации*, *тестирования*, *продажи* и *сопровождения*. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Классы безопасности

"Критерии ..." Министерства обороны США открыли путь к *ранжированию* информационных систем по *степени доверия* безопасности.

В "*Оранжевой книге*" 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 жесткие 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, ее *политика безопасности* и *уровень гарантированности* должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

Класс С1:

- *доверенная вычислительная база* должна управлять доступом именованных пользователей к именованным объектам;
- пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые *доверенной вычислительной базой*. Для *аутентификации* должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
- *доверенная вычислительная база* должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов *доверенной вычислительной базы* ;
- защитные механизмы должны быть протестированы на предмет соответствия их поведения *системной документации*. *Тестирование* должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты *доверенной вычислительной базы* ;
- должны быть описаны подходы к безопасности, используемые производителем, и применение этих подходов при *реализации доверенной вычислительной базы*.

Класс С2 (в дополнение к С1):

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов *доверенной вычислительной базы* необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
- *доверенная вычислительная база* должна создавать, поддерживать и защищать журнал *регистрационной информации*, относящейся к доступу к объектам, контролируемым базой;
- *тестирование* должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты *регистрационной информации*.

Класс B1 (в дополнение к C2):

- *доверенная вычислительная база* должна управлять *метками безопасности*, ассоциируемыми с каждым субъектом и хранимым объектом;
- *доверенная вычислительная база* должна обеспечить *реализацию принудительного управления доступом* всех субъектов ко всем хранимым объектам;
- *доверенная вычислительная база* должна обеспечивать взаимную *изоляцию процессов* путем *разделения* их *адресных пространств* ;
- группа специалистов, полностью понимающих *реализацию доверенной вычислительной базы*, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и *тестированию* ;
- должна существовать неформальная или *формальная модель политики безопасности*, поддерживаемой *доверенной вычислительной базой*.

Класс B2 (в дополнение к B1):

- снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;
- к *доверенной вычислительной базе* должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной *идентификации* и *аутентификации* ;
- должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
- *доверенная вычислительная база* должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;
- системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;
- должна быть продемонстрирована относительная устойчивость *доверенной вычислительной базы* к попыткам проникновения;
- модель *политики безопасности* должна быть формальной. Для *доверенной вычислительной базы* должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;
- в процессе разработки и *сопровождения доверенной вычислительной базы* должна использоваться система *конфигурационного управления*, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;
- тесты должны подтверждать действенность мер по уменьшению пропускной способности *тайных каналов передачи информации*.

Класс B3 (в дополнение к B2):

- для *произвольного управления доступом* должны обязательно использоваться *списки управления доступом* с указанием разрешенных режимов;
- должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу *политике безопасности* системы. *Администратор безопасности* должен немедленно извещаться о попытках нарушения *политики безопасности*, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом;
- *доверенная вычислительная база* должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
- процедура анализа должна быть выполнена для временных тайных каналов;
- должна быть специфицирована роль *администратора безопасности*. Получить права *администратора безопасности* можно только после выполнения явных, протоколируемых действий;
- должны существовать процедуры и/или механизмы, позволяющие произвести *восстановление после сбоя* или иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость *доверенной вычислительной базы* к попыткам проникновения.

Класс А1 (в дополнение к В3):

- *тестирование* должно продемонстрировать, что *реализация доверенной вычислительной базы* соответствует *формальным спецификациям верхнего уровня* ;
- помимо описательных, должны быть представлены *формальные спецификации верхнего уровня*. Необходимо использовать современные методы *формальной спецификации* и *верификации* систем;
- механизм *конфигурационного управления* должен распространяться на весь *жизненный цикл* и все компоненты системы, имеющие отношение к обеспечению безопасности;
- должно быть описано соответствие между *формальными спецификациями верхнего уровня* и исходными текстами.

Такова классификация, введенная в "*Оранжевой книге*". Коротко ее можно сформулировать так:

- уровень С - *произвольное управление доступом* ;
- уровень В - *принудительное управление доступом* ;
- уровень А - *верифицируемая* безопасность.

Рекомендации X.800
Сетевые сервисы безопасности

Следуя скорее исторической, чем предметной логике, мы переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее "*Оранжевой книги*", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (*сервисах) безопасности*, а также на необходимых для их *реализации* защитных механизмах.

Выделяют следующие *сервисы безопасности* и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как *маскарад* и повтор предыдущего сеанса связи. *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 упомянем **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. Побочным продуктом неотказуемости является **аутентификация источника данных**.

В следующей таблице указаны уровни **эталонной семиуровневой модели** OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Таблица 5.1. Распределение функций безопасности по уровням *эталонной семиуровневой модели* OSI

Функции безопасности	**Уровень**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

"+" данный уровень может предоставить функцию безопасности;
"-" данный уровень не подходит для предоставления функции безопасности.

Сетевые механизмы безопасности

Для *реализации* сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- **шифрование** ;
- **электронная цифровая подпись** ;
- механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
- механизмы *аутентификации*. Согласно рекомендациям X.800, *аутентификация* может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы **дополнения трафика** ;
- механизмы **управления маршрутизацией**. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять *метка безопасности*, ассоциированная с передаваемыми данными;
- механизмы **нотаризации**. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В следующей таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для *реализации* той или иной функции.

Таблица 5.2. Взаимосвязь функций и механизмов безопасности

Функции	**Механизмы**							
	Шифрование	**Электронная подпись**	**Управление доступом**	**Целостность**	**Аутентификация**	**Дополнение трафика**	**Управление маршрутизацией**	**Нотаризация**
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

"+" механизм пригоден для *реализации* данной функции безопасности;

"-" механизм не предназначен для *реализации* данной функции безопасности.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение **криптографических ключей**, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база *управления безопасностью*. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для *реализации* избранной *политики безопасности*.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование *сервисов безопасности*;
- администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим 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.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

управление ключами (генерация и распределение) ;

управление шифрованием (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается *криптографическими средствами*, также тяготеет к данному направлению;

администрирование управления доступом (*распределение информации*, необходимой для управления - паролей, списков доступа и т.п.);

управление *аутентификацией* (*распределение информации*, необходимой для *аутентификации* - паролей, ключей и т.п.);

управление *дополнением трафика* (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.);

управление маршрутизацией (выделение доверенных путей);

управление *нотаризацией* (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Основные понятия

По историческим причинам данный стандарт часто называют "*Общими критериями*" (или даже ОК). Мы также будем использовать это сокращение.

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты *оценки безопасности* ИС и порядок их использования. В отличие от "*Оранжевой книги*", ОК не содержат предопределенных *"классов безопасности"*. Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - **задания по безопасности**, типовые **профили защиты** и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; *оценка безопасности* тоже вышла на сопоставимый уровень сложности, и "*Общие критерии*" предоставили соответствующий *инструментарий*.

Важно отметить, что **требования могут быть параметризованы**, как и полагается библиотечным функциям.

Как и "*Оранжевая книга*", ОК содержат два основных вида **требований** безопасности:

функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

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

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки (ОО)** - совокупности программного, программно-аппаратного и/или аппаратного обеспечения, возможно сопровождаемая руководствами.

Профиль защиты - независимое от реализации изложение потребностей в безопасности для некоторого типа ОО.

Задание по безопасности - зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного ОО.

По ИСО/МЭК 15408 оценка ЗБ/ОО проходит в два этапа:

оценка ЗБ: на этом этапе определяют достаточность ОО и среды функционирования;

оценка ОО: на этом этапе определяют корректность ОО; как отмечалось ранее, оценка ОО не включает оценку корректности среды функционирования.

Оценку ЗБ выполняют путем применения критериев оценки заданий *по* безопасности (которые определены в разделе ASE ИСО/МЭК 15408-3). Конкретный способ применения критериев ASE определяется используемой методологией оценки.

В то время как ЗБ всегда описывает конкретный ОО (например, *межсетевой экран* X-2, версия 3.1), ПЗ предназначен для описания типа ОО (например, межсетевые экраны прикладного уровня). Поэтому один и тот же ПЗ можно использовать в качестве шаблона для *множества* различных ЗБ, которые будут использовать в различных оценках.

Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальным центром компьютерной безопасности США была опубликована *интерпретация* "*Оранжевой книги*" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются *сервисы безопасности*, специфичные или особенно важные для сетевых конфигураций.

В первой части вводится *минимум* новых понятий. Важнейшее из них - **сетевая доверенная вычислительная база**, распределенный аналог *доверенной вычислительной базы* изолированных систем. Сетевая *доверенная вычислительная база* формируется из всех частей всех компонентов сети, обеспечивающих информационную *безопасность*. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая *политика безопасности* реализовывалась, несмотря на *уязвимость* коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет *прямой* зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования *меток безопасности*, получается *сеть*, не удовлетворяющая требованию целостности меток. В качестве противоположного примера рассмотрим *объединение* двух компонентов, один из которых сам не обеспечивает *протоколирование* действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию *подотчетности*

Сетевая *конфигурация* должна быть *устойчива к отказам* отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит **криптография**, помогающая поддерживать как *конфиденциальность*, так и *целостность*. Следствием использования криптографических методов является необходимость *реализации* механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством *по* сравнению не только с "Оранжевой книгой", но и с рекомендациями X.800. *Сетевой сервис* перестает быть доступным, когда *пропускная способность* коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать *запросы. Удаленный ресурс* может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. *Доверенная система* должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

внесение в конфигурацию той или иной формы **избыточности** (резервное оборудование, запасные каналы связи и т.п.);

наличие средств **реконфигурирования** для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;

рассредоточенность сетевого **управления**, отсутствие **единой точки отказа** ;

наличие средств **нейтрализации отказов** (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);

выделение **подсетей** и **изоляция** групп **пользователей** друг от друга.

Подходы, принципы, методы и средства обеспечения безопасности

Под обеспечением безопасности информационных систем понимают меры, предохраняющие информационную систему от случайного или преднамеренного вмешательства в режимы ее функционирования. Существует два принципиальных подхода к обеспечению компьютерной безопасности.

Фрагментарный. Данный подход ориентируется на противодействие строго определенным угрозам при определенных условиях (например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д.). Достоинством фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Недостатком – локальность действия, т.е. фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов от конкретной угрозы.

Комплексный. Данный подход получил широкое распространение вследствие недостатков, присущих фрагментарному. Он объединяет разнородные меры противодействия угрозам и традиционно рассматривается в виде трех дополняющих друг друга направлений. Организация защищенной среды обработки информации позволяет в рамках существующей политики безопасности обеспечить соответствующий уровень безопасности АИС. Недостатком данного подхода является высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления


Факторы угроз информационной безопасности
Факторы угроз компьютерной безопасности
Управление защитой компьютерной безопасностью
Правовое обеспечение защиты компьютерной безопасности
Инженерно-техническое обеспечение защиты компьютерной
Организационное обеспечение защиты компьютерной безопасности


Управление защитой информации
Защита информационных ресурсов
Комплексная защита объектов
Обеспечение локальной безопасности
Предупреждение несанкционированных действий в отношении информации
Обеспечение физической и логической целостности информации
Защита от дезинформации
Обеспечение качества хранения информации

Особенностью системного подхода к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы.

Системный подход к защите информации базируется на следующих методологических принципах:

конечной цели – абсолютного приоритета конечной (глобальной) цели;

единства – совместного рассмотрения системы как целого' и как совокупности частей (элементов);

связности – рассмотрения любой части системы совместно с ее связями с окружением;

модульного построения – выделения модулей в системе и рассмотрения как совокупности модулей;

иерархии – введения иерархии частей (элементов) и их ранжирования;

функциональности – совместного рассмотрения структуры и функции с приоритетом функции над структурой;

развития – учета изменяемости системы, ее способности к развитию, расширению, замене частей, накапливанию информации;

децентрализации – сочетания в принимаемых решениях и управлении централизации и децентрализации;

неопределенности – учета неопределенностей и случайностей в системе.

Современные исследователи выделяют следующие методологические, организационные и реализационные принципы информационной (в том числе компьютерной) безопасности.

Принцип законности. Состоит в следовании действующему законодательству в области обеспечения информационной безопасности.

Принцип неопределенности. Возникает вследствие неясности поведения субъекта, т.е. кто, когда, где и каким образом может нарушить безопасность объекта защиты.

Принцип невозможности создания идеальной системы защиты. Следует из принципа неопределенности и ограниченности ресурсов указанных средств.

Принципы минимального риска и минимального ущерба. Вытекают из невозможности создания идеальной системы защиты. В соответствии с ним необходимо учитывать конкретные условия существования объекта защиты для любого момента времени.

Принцип безопасного времени. Предполагает учет абсолютного времени, т.е. в течение которого необходимо сохранение объектов защиты; и относительного времени, т.е. промежутка времени от момента выявления злоумышленных действий до достижения цели злоумышленником.

Принцип «защиты всех ото всех». Предполагает организацию защитных мероприятий против всех форм угроз объектам защиты, что является следствием принципа неопределенности. Принципы персональной ответственности. Предполагает персональную ответственность каждого сотрудника предприятия, учреждения и организации за соблюдение режима безопасности в рамках своих полномочий, функциональных обязанностей и действующих инструкций.

Принцип ограничения полномочий. Предполагает ограничение полномочий субъекта на ознакомление с информацией, к которой не требуется доступа для нормального выполнения им своих функциональных обязанностей, а также введение запрета доступа к объектам и зонам, пребывание в которых не требуется по роду деятельности.

Принцип взаимодействия и сотрудничества. Во внутреннем проявлении предполагает культивирование доверительных отношений между сотрудниками, отвечающими за безопасность (в том числе информационную), и персоналом. Во внешнем проявлении – налаживание сотрудничества со всеми заинтересованными организациями и лицами (например, правоохранительными органами).

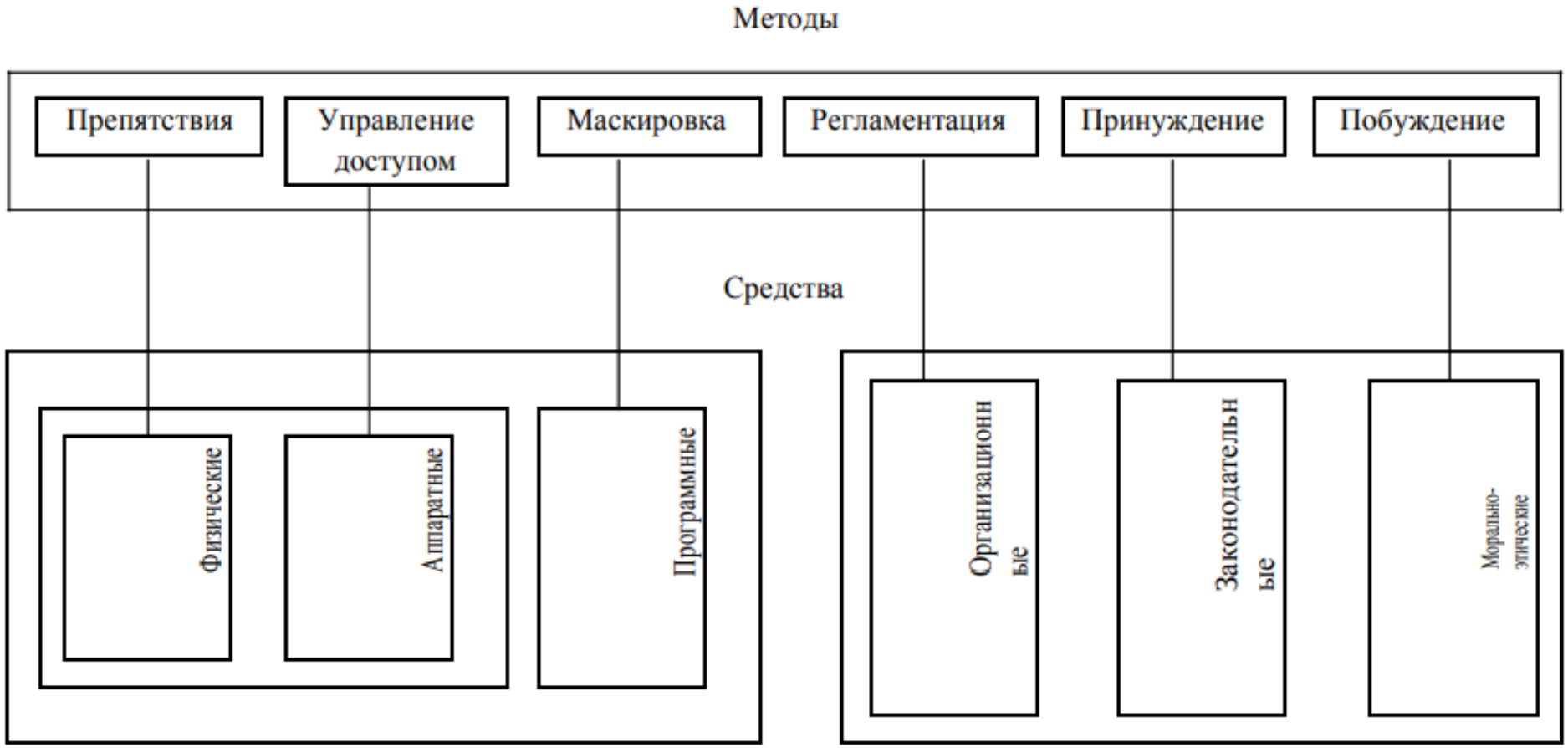
Принцип комплексности и индивидуальности. Подразумевает невозможность обеспечения безопасности объекта защиты каким-либо одним мероприятием, а лишь совокупностью комплексных, взаимосвязанных и дублирующих друг друга мероприятий, реализуемых с индивидуальной привязкой к конкретным условиям.

Принцип последовательных рубежей безопасности. Предполагает как можно более раннее оповещение о состоявшемся посягательстве на безопасность того или иного объекта защиты или ином неблагоприятном происшествии с целью увеличения вероятности того, что заблаговременный сигнал тревоги средств защиты обеспечит сотрудникам, ответственным за безопасность, возможность вовремя определить причину тревоги и организовать эффективные мероприятия по противодействию.

Принципы равнопрочности и равномощности рубежей защиты. Равнопрочность подразумевает отсутствие незащищенных участков в рубежах защиты. Равномощность предполагает относительно одинаковую величину защищенности рубежей защиты в соответствии со степенью угроз объекту защиты. Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты

Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки. Пользователям предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации. Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ЭИС без ее предварительной регистрации.

Обеспечение надежности системы защиты, т.е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала. Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты. Экономическая целесообразность использования систем защиты. Она выражается в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту случае разработки и эксплуатации АИС без системы защиты информации


Методы
Препятствия
Управление доступом
Маскировка
Регламентация
Принуждение
Побуждение
Средства
Физические
Аппаратные
Программные
Организационные
Законодательные
Морально-этические

Методами обеспечения защиты информации на предприятии являются следующие:

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).

Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
- аутентификацию (установления подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- регистрацию обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе при попытках несанкционированных действий)

Маскировка – метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Принуждение – метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

Побуждение – метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Аппаратные средства защиты – это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля

Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития.

Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия.

Аппаратно-программные средства защиты – средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы. Криптографические средства – средства защиты с помощью преобразования информации (шифрование).

Организационные средства – организационно-технические и организационноправовые мероприятия по регламентации поведения персонала.

Законодательные средства – правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.

Морально-этические средства – нормы, традиции в обществе, например: Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ в США.

Для реализации мер безопасности используются различные механизмы шифрования (криптографии).

Криптография – это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений. Сущность криптографических методов заключается в следующем. Готовое к передаче сообщение – будь то данные, речь либо графическое изображение того или иного документа, обычно называется открытым, или незащищенным текстом.

В процессе передачи такого сообщения по незащищенным каналам связи оно может быть легко перехвачено или отслежено подслушивающим лицом посредством умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к сообщению оно зашифровывается, преобразуясь в шифрограмму, или закрытый текст.

Санкционированный пользователь, получив сообщение, дешифрует или раскрывает его посредством обратного преобразования криптограммы. Вследствие чего получается исходный открытый текст.

Шифрование может быть симметричным и асимметричным. Первое основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Второе характеризуется тем, что для шифрования используется один общедоступный ключ, а для дешифрования – другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Наряду с шифрованием внедряются следующие механизмы безопасности:

- цифровая электронная подпись;
- контроль доступа;
- обеспечение целостности данных;
- обеспечение аутентификации;
- постановка трафика;
- управление маршрутизацией;
- арбитраж или освидетельствование

Механизмы цифровой подписи основываются на алгоритмах ассиметричного шифрования и включают две процедуры: формирование подписи отправителем и ее опознавание получателем.

Первая процедура обеспечивает шифрование блока данных либо его дополнение криптографической, контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя. Механизмы контроля доступа осуществляют проверку полномочий объектов АИС (программ и пользователей) на доступ к ресурсам сети.

При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке. Механизмы обеспечения целостности данных применяются к отдельному блоку и к потоку данных.

Целостность блока является необходимым, но не достаточным условием целостности потока и обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

Механизмы постановки трафика, называемые также механизмами заполнения текста, используют для засекречивания потока данных. Они основываются на генерации объектами АИС блоков, их шифровании и организации передачи по каналам сети. Тем самым нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам. Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами АИС, третьей стороной.

Для этого вся информация, отправляемая или получаемая объектами, проходит через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики

Отметим типичные недостатки, присущие системе безопасности объектов:

- узкое, несистемное понимание проблемы безопасности объекта;
- пренебрежение профилактикой угроз, работа по принципу «Появилась угроза – начинаем ее устранять»;
- некомпетентность в безопасности, неумение сопоставлять затраты и результаты;
- «технократизм» руководства и специалистов службы безопасности, интерпретация всех задач на языке знакомой им области.

Спасибо за внимание!