**Лекция №2: Основы информационной безопасности**

**Цель:** дать студентам представление об основных понятиях информационной безопасности, раскрыть сущность, задачи и компоненты системы защиты информации, а также сформировать понимание угроз информационной безопасности и методов их предотвращения.

### 1.1. Основные понятия информационной безопасности

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое *информационная безопасность*. Термин "*информационная безопасность*" может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под **информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* *субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры [[1](https://www.intuit.ru/studies/courses/697/553/literature" \l "literature.1)].

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

* **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
* **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
* **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

**Угрозы информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [[2](https://www.intuit.ru/studies/courses/697/553/literature" \l "literature.2),[3](https://www.intuit.ru/studies/courses/697/553/literature" \l "literature.3)]. **Атакой**называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

*Угроза* является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

* по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
* по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
* по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
* по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
2. административный – комплекс мер, предпринимаемых локально руководством организации;
3. процедурный уровень – меры безопасности, реализуемые людьми;
4. *программно-технический уровень* – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

### 1.2. Закона РК "Об информации, информационных технологиях и о защите информации"

Одним из ключевых законов в области защиты информации является **Закон Республики Казахстан "Об информации, информационных технологиях и о защите информации"** от 27 июля 2006 года № 149. Этот закон регулирует отношения в сфере использования информационных технологий, защиты информации, а также установление прав и обязанностей субъектов, связанных с обработкой и защитой информации.

Некоторые основные моменты и понятия, закрепленные в этом законе, которые требуют пристального рассмотрения:

1. **Информация** - любые сведения, независимо от формы их представления, которые могут быть использованы, обработаны и переданы для достижения определенной цели.
2. **Информационные технологии** - это совокупность методов, средств и организационных мер, направленных на сбор, обработку, хранение и распространение информации.
3. **Защита информации** - комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности информации в процессе ее хранения, обработки и передачи.
4. **Персональные данные** - любая информация, относящаяся к физическому лицу, которое может быть идентифицировано на основе этих данных. Закон регулирует их защиту, включая права субъектов данных и обязанности операторов.
5. **Операторы информации** - физические и юридические лица, государственные органы, которые организуют или осуществляют обработку информации, в том числе персональных данных, и несут ответственность за соблюдение требований по ее защите.
6. **Конфиденциальность информации** - это соблюдение принципа, согласно которому информация не доступна несанкционированным лицам, и доступ к ней осуществляется только на основании соответствующего разрешения.
7. **Информационные системы** - организованные совокупности данных и информационных технологий, которые используются для обработки и защиты информации.
8. **Управление доступом** - установление правил доступа к информации для различных субъектов, с учетом уровня доверия, прав доступа и целей использования.
9. **Ответственность за нарушение защиты информации** - в том числе штрафы, приостановка деятельности и другие санкции в случае несанкционированного доступа, утечек данных и других нарушений.

Закон также регулирует многие аспекты, связанные с **криптографией**, **информационной безопасностью**, а также **защищенность электронных данных**.

Основное внимание уделяется обеспечению безопасности данных и предотвращению несанкционированного доступа, утечек и их незаконного использования. В этой связи особое значение имеют положения закона, касающиеся обязательств операторов по защите информации и ответственности за нарушения в этой области.

Для успешного соблюдения закона и обеспечения безопасного обращения с информацией организации и физические лица должны четко понимать свои права и обязанности, а также строго следовать установленным стандартам безопасности и нормативам.

Закон регулирует отношения, возникающие при:

* осуществлении права на поиск, получение, передачу, производство и распространение информации;
* применении информационных технологий;
* обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

* **информация**- сведения (сообщения, данные) независимо от формы их представления;
* **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
* **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
* **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
* **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
* **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [[4](https://www.intuit.ru/studies/courses/697/553/literature" \l "literature.4)].

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных законами;
4. равноправие языков народов Республики Казахстан при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Республики Казахстан при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена законами.

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1. информацию, свободно распространяемую;
2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. информацию, которая в соответствии с законами подлежит предоставлению или распространению;
4. информацию, распространение которой в Республике Казахстан ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Республики Казахстан, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. своевременное обнаружение фактов несанкционированного доступа к информации;
3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, РК "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РК и определяет *права* и обязанности его субъектов.

### 1.3 Триада безопасной ИТ-инфраструктуры – Конфиденциальность, Целостность, Доступность

Основой безопасной ИТ-инфраструктуры является триада сервисов – *Конфиденциальность*, *Целостность*, Доступность – *Confidentiality*, *Integrity*, *Availability* (*CIA*).

Целью информационной безопасности является обеспечение трех наиболее важных сервисов безопасности: *конфиденциальность*, *целостность* и доступность.

*Конфиденциальность* – это гарантия, что *информация* может быть прочитана и проинтерпретирована только теми людьми и процессами, которые авторизованы это делать. Обеспечение конфиденциальности включает процедуры и меры, предотвращающие *раскрытие информации* неавторизованными пользователями. *Информация*, которая может считаться конфиденциальной, также называется чувствительной. Примером может являться почтовое сообщение, которое защищено от прочтения кем бы то ни было, кроме адресата.

*Целостность* – это гарантирование того, что *информация* остается неизменной, корректной и аутентичной. Обеспечение целостности предполагает предотвращение и *определение* неавторизованного создания, модификации или удаления информации. Примером могут являться меры, гарантирующие, что почтовое сообщение не было изменено при пересылке.

***Доступность*** – это гарантирование того, что авторизованные пользователи могут иметь *доступ* и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая *производительность*. Обеспечение доступности включает меры для поддержания доступности информации, несмотря на возможность создания помех, включая отказ системы и преднамеренные попытки нарушения доступности. Примером может являться *защита доступа* и обеспечение пропускной способности почтового сервиса.

Три основных сервиса – *CIA* – служат фундаментом информационной безопасности. Для реализации этих трех основных сервисов требуется выполнение следующих сервисов.

***Идентификация*** – сервис, с помощью которого указываются уникальные атрибуты пользователей, позволяющие отличать пользователей друг от друга, и способы, с помощью которых пользователи указывают свои идентификации информационной системе. *Идентификация* тесно связана с аутентификацией.

***аутентификация*** – сервис, с помощью которого доказывается, что участники являются требуемыми, т.е. обеспечивается *доказательство* идентификации. Это может достигаться с помощью паролей, смарт-карт, биометрических токенов и т.п. В случае передачи единственного сообщения *аутентификация* должна гарантировать, что получателем сообщения является тот, кто нужно, и сообщение получено из заявленного источника. В случае установления соединения имеют *место* два аспекта. Во-первых, при инициализации соединения сервис должен гарантировать, что оба участника являются требуемыми. Во-вторых, сервис должен гарантировать, что на соединение не воздействуют таким образом, что третья сторона сможет маскироваться под одну из легальных сторон уже после установления соединения.

Подотчетность – возможность системы идентифицировать отдельного индивидуума и выполняемые им действия. Наличие этого сервиса означает возможность связать действия с пользователями. Данный сервис очень тесно связан с сервисом невозможности отказа.

Невозможность отказа – сервис, который обеспечивает невозможность индивидуума отказаться от своих действий. Например, если потребитель сделал заказ, и в системе отсутствует сервис невозможности отказа, то потребитель может отказаться от факта покупки. Невозможность отказа обеспечивает способы доказательства того, что *транзакция* имела *место*, не зависимо от того, является ли *транзакция* online-заказом или почтовым сообщением, которое было послано или получено. Для обеспечения невозможности отказа как правило используются цифровые подписи.

***Авторизация*** – *права* и разрешения, предоставленные индивидууму (или процессу), которые обеспечивают возможность доступа к ресурсу. После того, как *пользователь* аутентифицирован, *авторизация* определяет, какие *права доступа* к каким ресурсам есть у пользователя.

Защита частной информации – уровень конфиденциальности, который предоставляется пользователю системой. Это часто является важным компонентом безопасности. Защита частной информации не только необходима для обеспечения конфиденциальности данных организации, но и необходима для защиты частной информации, которая будет использоваться оператором.

Если хотя бы один из этих сервисов не функционирует, то можно говорить о нарушении всей исходной триады *CIA*.

Для реализации сервисов безопасности должна быть создана так называемая "оборона в глубину". Для этого должно быть проделано:

1. Необходимо обеспечить гарантирование выполнения всех сервисов безопасности.
2. Должен быть выполнен *анализ рисков*.
3. Необходимо реализовать аутентификацию и управление *Идентификациями.*
4. Необходимо реализовать *авторизацию* доступа к ресурсам.
5. Необходимо обеспечение подотчетности.
6. Необходимо гарантирование доступности всех сервисов системы.
7. Необходимо управление конфигурацией.
8. Необходимо управление инцидентами.

### 1.4 Гарантирование выполнения

Обеспечение выполнения сервисов безопасности выполнить следующее:

* Разработать организационную политику безопасности.
* Рассмотреть существующие нормативные требования и акты.
* Обеспечить обучение сотрудников, ответственных за ИБ.

Гарантирование выполнения, наряду с анализом рисков, является одной из самых важных *компонент*, обеспечивающих создание обороны в глубину. Это является основой, на которой построены многие другие компоненты. Оценка гарантированности выполнения может во многом определять все состояние и уровень зрелости надежной инфраструктуры.

Организационная политика содержит руководства для пользователей и администраторов. Эта политика должна быть четкой, ясной и понимаемой не только техническими специалистами. Политика должна охватывать не только текущие условия, но и определять, что и как должно быть сделано, если произошла *атака*.

### 1.5 Анализ рисков

При *анализе рисков* первым делом следует проанализировать информационные *активы*, которые должны быть защищены.

Любое обсуждение риска предполагает *определение* и оценку информационных активов. Актив – это все, что важно для организации. Критический актив – это актив, который жизненно важен для функционирования организации, ее репутации и дальнейшего развития.

***Анализ рисков*** является процессом определения рисков для информационных активов и принятия решения о том, какие риски являются приемлемыми, а какие нет. *Анализ рисков* включает:

* Идентификацию и приоритезацию информационных активов.
* Идентификацию и категоризацию угроз этим активам.
* Приоритезацию рисков, т.е. определение того, какие риски являются приемлемыми, какие следует уменьшить, а какие избегать.
* Уменьшение рисков посредством использования различных сервисов безопасности.

Угрозой является любое событие, которое может иметь нежелательные последствия для организации. Примерами угроз являются:

* Возможность раскрытия, модификации, уничтожения или невозможность использования информационных активов.
* Проникновение или любое нарушение функционирования информационной системы. Примерами могут быть:
  + Вирусы, черви, троянские кони.
  + DoS-атаки.
  + Просмотр сетевого трафика.
  + Кража данных.
* Потеря информационных активов в результате наличия единственной точки отказа. Примерами могут быть:
  + Критичные данные, для которых нет резервной копии.
  + Единственное критичное место в сетевой инфраструктуре (например, базовый маршрутизатор).
  + Неправильное управление доступом к ключам, которые используются для шифрования критических данных.

Уязвимости, которые могут существовать в информационных активах, могут быть связаны с наличием:

* Слабых мест в ПО:
  + Использование установок по умолчанию (учетные записи и пароли по умолчанию, отсутствие управления доступом, наличие необязательного ПО).
  + Наличие ошибок в ПО.
  + Некорректная обработка входных данных.
* Слабых мест в архитектуре:
  + Наличие единственной точки отказа.
* Слабых мест, связанных с человеческим фактором.

Возможные стратегии управления рисками:

1. Принять риск. В этом случае организация должна иметь полное представление о потенциальных угрозах и уязвимостях для информационных активов. В этом случае организация считает, что риск не является достаточным, чтобы защищаться от него.
2. Уменьшить риск.
3. Передать риск. Организация решает заключить соглашение с третьей стороной для уменьшения риска.
4. Избежать риск.

### 1.6 Аутентификация и управление Идентификациями

*Идентификация* пользователя дает возможность вычислительной системе отличать одного пользователя от другого и обеспечивать высокую *точность* управления доступом к сервисам и ресурсам. Идентификации могут быть реализованы разными способами, такими как пароли, включая одноразовые, цифровые сертификаты, биометрические параметры. Возможны разные способы хранения идентификаций, такие как *базы данных*, ***LDAP***, смарт-карты.

Система должна иметь возможность проверить действительность (*аутентичность*) предоставленной идентификации. Сервис, который решает эту проблему, называется аутентификацией.

Термин сущность (*entity*) часто лучше подходит для обозначения предъявителя идентификации, чем термин *пользователь*, так как участниками аутентификационного процесса могут быть не только пользователи, но и программы и аппаратные устройства, например, веб-серверы или маршрутизаторы.

Разные требования к безопасности требуют разных методов идентификации и аутентификации. Во многих случаях бывает достаточно обеспечивать *безопасность* с помощью имени пользователя и пароля. В некоторых случаях необходимо использовать более сильные методы аутентификации.

Возможны следующие способы аутентификации.

#### 1.6.1 Пароли

Наиболее часто используемой формой идентификации на сегодняшний день является имя пользователя и пароль. Причины этого в том, что, во-первых, пользователи сами могут выбрать пароли, которые им легко запомнить, а всем остальным трудно отгадать, а, во-вторых, данный способ аутентификации требует минимальных административных усилий.

Однако использование паролей имеет определенные проблемы. Любой пароль, который является словом из некоторого словаря, может быть сравнительно быстро найден с помощью программ, которые перебирают пароли. Пароль, состоящий из случайных символов, трудно запомнить.

В большинстве современных приложений пароль не хранится и не передается в явном виде.

#### 1.6.2 Токены

Вместо того, чтобы в качестве идентификации использовать нечто, что кто-то знает, можно использовать нечто, что он имеет. Обычно под токенами понимаются некоторые аппаратные устройства, которые предъявляет пользователь в качестве аутентификации. Такие устройства позволяют пользователям не запоминать пароли. Примерами таких токенов являются:

* Смарт-карты.
* Одноразовые пароли.
* Устройства, работающие по принципу запроса – ответа.

#### 1.6.3 Биометрические параметры

Используются некоторые физические характеристики пользователя.

#### 1.6.4 Криптографические ключи

Криптография предоставляет способы, с помощью которых сущность может доказать свою идентификацию. Для этого она использует ключ, являющийся строкой битов, который подается в алгоритм, выполняющий шифрование данных. На самом деле ключ аналогичен паролю – это нечто, что сущность знает.

Существует два типа алгоритмов и, соответственно, два типа ключей – симметричные и асимметричные.

В случае использования асимметричных ключей необходимо развертывание инфраструктуры открытых ключей.

Во многих протоколах для взаимной аутентификации сторон могут использоваться ключи разных типов, т.е. одна из сторон аутентифицирует себя с помощью цифровой подписи (асимметричные ключи), а противоположная сторона – с помощью симметричного ключа (или пароля).

#### 1.6.5 Многофакторная аутентификация

В современных системах все чаще используется многофакторная *аутентификация*. Это означает, что аутентифицируемой сущности необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия.

#### 1.6.6 Централизованное управление идентификационными и аутентификационными данными

Для выполнения аутентификации для входа в сеть часто используются механизмы, обеспечивающие централизованную аутентификацию пользователя. Преимущества этого:

* Легкое администрирование.
* Увеличение производительности.

Примерами являются:

* Сервисы Директории:
  + Microsoft AD.
  + Различные реализации LDAP.
* Протоколы:
  + Radius.
  + PAP, CHAP.
  + Kerberos.
* Системы Казахстанской идентификации.

Целями систем идентификации являются:

* Обеспечить единую аутентификацию (так называемый Single Sign On – SSO) в пределах сетевого периметра или домена безопасности.
* Обеспечить пользователей возможностью легко управлять своими идентификационными данными.
* Создать родственные группы, которые могут доверять друг другу аутентифицировать своих пользователей.

### 1.7 Управление доступом

*Управление доступом* или *авторизация* означает *определение* прав и разрешений пользователей *по* доступу к ресурсам.

* Авторизация может быть реализована на уровне приложений, файловой системы и сетевого доступа.
* Принципы предоставления прав и разрешений должны определяться политикой организации.

Основные вопросы, на которые должен отвечать сервис авторизации: "Кто и что может делать в компьютерной системе или сети?" и "Когда и где он может это делать?".

Компоненты управления доступом:

Субъекты – *пользователь*, аппаратное устройство, процесс ОС или прикладная система, которым требуется *доступ* к защищенным ресурсам. *Идентификация* субъекта подтверждается с помощью механизмов аутентификации.

Объекты или ресурсы –файлы или любые сетевые ресурсы, к которым субъект хочет получить *доступ*. Это включает файлы, папки и другие типы ресурсов, такие как записи *базы данных* (*БД*), *сеть* или ее компоненты, например, принтеры.

Разрешения – *права*, предоставленные субъекту *по* доступу к данному объекту или ресурсу.

*Управление доступом* означает предоставление доступа к конкретным информационным активам только для авторизованных пользователей или групп, которые имеют право просматривать, использовать, изменять или удалять информационные *активы*. В сетевом окружении *доступ* может контролироваться на нескольких уровнях: на уровне файловой системы, на прикладном уровне или на сетевом уровне.

*Управление доступом* на уровне файловой системы может быть интегрировано в ОС. Как правило в этом случае используются *списки управления доступом* (Access *Control* *List* – *ACL*) или возможности (capabilities).

В случае использования *ACL* для каждого объекта создается *список*, в котором перечислены пользователи и их *права доступа* к данному объекту. В случае использования возможностей в системе хранится *список* разрешений для каждого пользователя.

При управлении доступом на сетевом уровне для разграничения трафика используются сетевые устройства.

При управлении доступом на сетевом уровне *сеть* может быть разбита на отдельные *сегменты*, *доступ* к которым будет контролироваться. Сегментацию на сетевом уровне можно сравнить с использованием управления доступом на уровне групп или ролей в файловой системе. Такое *деление* может быть основано на бизнес-задачах, необходимых сетевых ресурсах, выполняемых операциях (например, производственные сервера и тестовые сервера) или важности хранимой информации. Существует несколько способов сегментации сети. Двумя основными способами является использование маршрутизаторов и межсетевых экранов.

Маршрутизаторы являются шлюзами в *интернет* или делят внутреннюю *сеть* на различные *сегменты*. В этом случае маршрутизаторы выполняют различные политики разграничения трафика.

Межсетевыми экранами являются устройствами, просматривающими входящий и исходящий трафик и блокирующими пакеты в соответствии с заданными правилами.

Преимущества управления доступом на сетевом уровне:

* Возможное четкое определение точек входа, что облегчает мониторинг и управление доступом.
* Возможно скрытие внутренних адресов для внешних пользователей. Межсетевой экран может быть сконфигурирован как прокси или может выполнять преобразование адресов (Network Address Translation – NAT) для сокрытия внутренних IP-адресов хостов.

Недостатки управления доступом на сетевом уровне:

* Не всегда удается использовать подход "установить и забыть" – необходимо анализировать и изменять правила межсетевого экрана при изменении конфигурации или требований к безопасности.
* Может оказаться единственной точкой отказа.
* Анализирует только заголовки сетевого уровня.

*Управление доступом* на прикладном уровне предполагает использование разрешений и применение правил для доступа к приложениям и прикладным данным. В этом случае часто используются прокси-серверы.

Прокси-*сервер* является устройством или сервисом, который расположен между клиентом и целевым сервером. *Запрос* на *сервер* посылается к прокси-серверу. Прокси-*сервер* анализирует *запрос* и определяет, является ли он допустимым.

Преимущества управления доступом на прикладном уровне:

* Управление доступом отражает специфику конкретной целевой системы. Увеличивает точность (гранулированность) управления доступом.
* Может снизить влияние неправильной конфигурации отдельных хостов.
* Выполняется подробный анализ пакетов.
* Выполняется более сильная *аутентификация*.

Недостатки управления доступом на прикладном уровне:

* Прокси специфичны для приложений.
* Возможна несовместимость приложений с прокси. В этом случае можно только либо разрешать весть трафик, либо запрещать весь трафик.
* Высокая вычислительная нагрузка и, как следствие, возможно снижение производительности.

### 1.8 Обеспечение отчетности

Отчетность – это возможность знать, кто и что делал в системе и сети. Это включает:

* Создание и аудит системных логов.
* Мониторинг систем и сетевого трафика.
* Обнаружение проникновений.

Обеспечение отчетности позволяет знать, что происходит в компьютерных системах или сетях. Это может быть реализовано многими способами, но наиболее часто используются следующие:

* Конфигурирование системы таким образом, чтобы записывалась интересующая активность, такая как попытки входа пользователей в систему или сеть (успешные или не успешные).
* Инспектирование использования сети для определения типов сетевого трафика и его объема.
* Автоматический мониторинг систем для определения отключений сервисов.
* Использование систем обнаружения вторжений для оповещения администраторов о нежелательной активности в компьютерных системах или сетях.

При использовании подобных технологий важно правильно рассчитать количество необходимых ресурсов и время, необходимое для анализа собранных данных.

### 1.9 Гарантирование доступности

Гарантирование доступности состоит в определении точек возможного сбоя и ликвидации этих точек. Стратегии уменьшения негативных последствий отказов могут быть управленческие и технологические.

Первым делом следует определить потенциальные точки отказа в сетевой инфраструктуре. Такие критически важные устройства, как коммутаторы и маршрутизаторы, а также базовые с точки зрения функционирования серверы, такие как DNS-серверы, должны быть проанализированы с точки зрения возможного отказа и влияния этого на возможности функционирования ИТ. Это связано с управлением рисками – определить и минимизировать степень риска.

С точки зрения гарантирования доступности можно дать следующие определения.

Надежность – способность системы или отдельной компоненты вы-полнять требуемые функции при определенных условиях в указанный период времени.

*Избыточность* – создание одной или нескольких копий (*backup*) си-стемы, которые становятся доступными в случае сбоя основной системы, или наличие дополнительных возможностей системы для организации её отказоустойчивости.

*Отказоустойчивость* – способ функционирования, при котором функции *компонент* системы (такие как *процессор*, *сервер*, *сеть* или *БД*) выполняются дублирующими компонентами при отказе или плановом останове основных *компонент*. Способность системы или компонента продолжать нормально функционировать при отказе *ПО* или аппаратуры.

Необходимо проанализировать возможные точки отказа в следующих компонентах: данные, компоненты систем, сетевая *топология*, маршрутизаторы и коммутаторы, отдельные критичные сервисы.

Основные технологии обеспечения отказоустойчивости этих компо-нент:

* Данные:
  + Защита с помощью RAID.
  + Шифрование данных и управление ключом.
  + Стратегии создания копий и восстановления.
* Компоненты систем:
  + Горячее резервирование аппаратуры и подсистем.
  + Резервирование на уровне сетевых интерфейсов.
  + Резервирование данных на уровне ОС и приложений.
* Сетевая топология:
  + Обеспечение масштабируемости пропускной способности и количества интерфейсов.
* Маршрутизаторы и коммутаторы:
  + Использование протоколов, поддерживающих автоматиче-ское восстановление, таких как протоколы динамической маршрутизации, обладающие достаточной сходимостью и передающие минимальное количество служебной инфор-мации.
* Критические сервисы:
  + Обеспечение балансировки нагрузки для таких критических сервисов, как DNS, DHCP и т.п.
  + Обеспечение балансировки нагрузки для прикладных сер-веров (веб, почта, БД).
  + Обеспечение балансировки нагрузки для сетевых устройств, таких как межсетевые экраны и прокси-серверы.

### 1.10 Управление конфигурациями

При управлении конфигурациями необходимо обеспечить следующее:

* Регулярное обновление ПО.
* Управление и контроль существующих ресурсов.
* Управление изменениями.
* Оценка состояния сетевой безопасности.

Управление конфигурациями означает ежедневное использование проактивных технологий, которые гарантируют корректное функционирование ИТ-систем.

Управление обновлением *ПО* является одной из ежедневных обязанностей, которая является относительно простой. В идеале обновление должно проводиться на отдельном оборудовании и после тестирования переноситься на все производственные системы. Этого достаточно трудно добиться даже в небольших сетях. Различные производители, такие как Microsoft, и системы с открытым кодом, такие как Linux, уделяют большое внимание этой проблеме, и на сегодняшний день существуют достаточно зрелые технологии, например, *Windows Server* *Update* Services (WSUS), которые позволяют администратору управлять внесением обновлений в сетях, построенных с использованием ОС *Windows*. С другой стороны, для таких устройств сетевой инфраструктуры, как коммуникаторы и маршрутизаторы, обновление выполняется значительно труднее. Обычно они либо пол-ностью заменяются, либо должен быть загружен и заменен образ всей ОС.

*Эффективное управление* существующими ресурсами само *по* себе требует больших усилий. Все изменения конфигураций основных серверов и систем должны быть тщательно документированы.

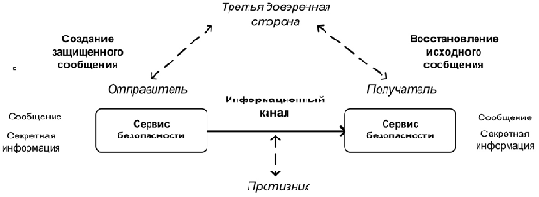
Также важна регулярная оценка состояния сетевой безопасности. Существуют различные инструментальные средства, такие как *Baseline* *Security* *Analyzer* компании Microsoft и инструментальное средство с открытым кодом Nessus, которые помогают администратору выполнить такую оценку.

### 1.11 Управление инцидентами

Регулярно происходят какие-либо события, относящиеся к безопасности. При возникновении компьютерного инцидента важно иметь эффективные способы его распознавания. Скорость, в которой можно распознать, проанализировать и ответить на инцидент, позволяет уменьшить *ущерб*, нанесенный инцидентом.

### 1.12 Использование третьей доверенной стороны

Модель безопасного сетевого взаимодействия в общем виде можно представить следующим образом:

[](https://www.intuit.ru/EDI/03_01_18_12/1514931930-14492/tutorial/1334/objects/3/files/8.png)

[увеличить изображение](https://www.intuit.ru/EDI/03_01_18_12/1514931930-14492/tutorial/1334/objects/3/files/8.png)  
**Рис. 1.8.**Использование третьей доверенной стороны

В некоторых случаях для выполнения сервисов безопасности необходимо взаимодействие с третьей доверенной стороной (Third Trusted *Party* – *TTP*). Например, третья сторона может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы доступна оппоненту. Либо третья сторона может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

### 1.13 Криптографические механизмы безопасности

Перечислим основные криптографические *механизмы* безопасности:

Алгоритмы *симметричного шифрования* – *алгоритмы шифрования*, в которых для шифрования и расшифрования используется один и тот же *ключ*.

Алгоритмы *асимметричного шифрования* – *алгоритмы шифрования*, в которых для шифрования и расшифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная открытый *ключ*, определить закрытый вычислительно трудно.

*Хэш-функции* – функции, входным значением которых является сообщение произвольной длины, а выходным значением – сообщение фиксированной длины. Хэш-функции обладают рядом свойств, которые позволяют с высокой долей вероятности определять изменение входного сообщения.

**Вопросы для закрепления материала**:

1. Что такое информационная безопасность и какие угрозы могут нарушать ее целостность?
2. Как ГОСТ "Защита информации. Основные термины и определения" определяет понятие информационной безопасности?
3. Какие три ключевых аспекта характеризуют информационную безопасность и как они влияют на защищенность данных?
4. Чем отличаются уязвимости и угрозы в контексте информационной безопасности?
5. Перечислите различные классификации угроз информационной безопасности.
6. В чем заключается отличие между случайными и преднамеренными угрозами?
7. Что является основным фактором, создающим угрозу информационной безопасности?
8. Приведите примеры угроз, нацеленных на конфиденциальность, целостность и доступность информации.
9. Опишите ключевые уровни защиты информации.
10. Как законодательный уровень влияет на систему защиты информации?
11. Какие меры безопасности могут быть реализованы на административном уровне для защиты информации?
12. Какие программно-технические средства обеспечивают защиту данных?
13. Какие ключевые понятия из Закона РК "Об информации, информационных технологиях и о защите информации" вы считаете наиболее важными для обеспечения безопасности данных?
14. Что подразумевает защита информации по Закону РК и какие меры предпринимаются для обеспечения конфиденциальности, целостности и доступности информации?
15. Какие обязанности накладывает Закон на операторов информационных систем?
16. Как законодательство регулирует сбор, обработку и распространение информации?
17. Что такое триада безопасности (CIA) и как она влияет на защиту информации?
18. Приведите примеры, иллюстрирующие каждый из аспектов триады: конфиденциальность, целостность, доступность.
19. Какова роль аутентификации и авторизации в обеспечении безопасности информации?
20. В чем заключается принцип "обороны в глубину" и как он применяется на практике для обеспечения информационной безопасности?
21. Как можно реализовать защиту информации от несанкционированного доступа и утечек данных?
22. Какие меры могут быть предприняты для предотвращения потери целостности данных?
23. Каковы основные принципы защиты персональных данных согласно Закону РК?