Тема 3.1 Информационная этика и право.

Информационная безопасность.

Безопасность – это не только наука, которую надо изучать, не только мастерство, секреты которого надо постигать, но это и культура, которую надо воспитывать**.**

Безопасность является той сферой, с которой любой человек сталкивается на протяжении всей жизни, в той или иной форме, на том или ином участке профессиональной деятельности. Организация защиты не может быть уделом только профессионалов. Те, кто выступает в качестве пользователей, исполнителей, носителей защищаемых сведений, в отношении которых осуществляется физическая охрана, должны разбираться в вопросах безопасности не хуже тех, кто ее обеспечивает.[1]

В.Даль указывал, что безопасность есть отсутствие опасности, сохранность, надежность. По С.Ожегову, безопасность – это «состояние, при котором не угрожает опасность, есть защита от опасности». Сегодня появилось множество других определений безопасности, авторы которых исходят из разных критериев. Также полагают, что «безопасность есть состояние, тенденции развития (в том числе латентные) и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно обусловленными инновациями и свободное, соответствующее собственной природе и ею определяемое функционирование**».**

Начнем изучение этой темы с определений в терминологии информационной безопасности.

Информационная безопасность — механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;

- целостность: достоверность и полноту информации и методов ее обработки;

- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости**.**

Под ***информационной безопасностью*** Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Исходя из Доктрины информационной безопасности Российской Федерации следует что:

- Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и

[1] Организация систем защиты информации. Учебно-методическое пособие. Е.В.Морозова. – М.: Школа охраны «Баярд», 2003 – 96 с.

интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

- Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.
- Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения.

Основными составляющими и аспектами информационной безопасности (которые не следует отождествлять с информационной безопасностью в целом) являются:

- Защита информации (в смысле охраны персональных данных);
- Компьютерная безопасность или безопасность данных;
- Защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий;
- Информационно-психологическая удовлетворенность потребностей граждан и защищенность от негативных информационно-психологических и информационно-технических воздействий.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что ***информационная безопасность*** есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Угрозы информационной безопасности

Под ***угрозой (threat)*** понимаются характеристики, свойства системы и окружающее среды, которые в соответствующих условиях могут вызвать появление опасного события.

Угроза - это потенциальная возможность определенным образом

нарушить информационную безопасность. Попытка реализации *угрозы* называется ***атакой***, а тот, кто предпринимает такую попытку, - ***злоумышленником***. Потенциальные злоумышленники называются ***источниками угрозы***.

Существует три разновидности угроз:

1. ***Угроза нарушения конфиденциальности*** заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

2. ***Угроза нарушения целостности,*** которая включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Целостность информации это существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее неискаженности.

3. ***Угроза отказа служб*** возникающая всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Исходя из Доктрины информационной безопасности Российской Федерации угрозы информационной безопасности Российской Федерации подразделяются на **следующие виды**:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Уровни 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.

Направления защиты компьютерной информации.

Основными целями и направлениями защиты данных провозглашаются предотвращение потери и искажения данных, несанкционированного использования, угрозы безопасности человеку и государству, защита прав субъектов информатизации. Защита должна производиться как в интересах держателей информации (собственников, владельцев, пользователей), так и людей, имеющих непосредственное отношение к ним (авторов, пациентов медицинских учреждений, коммерсантов и т.д.).

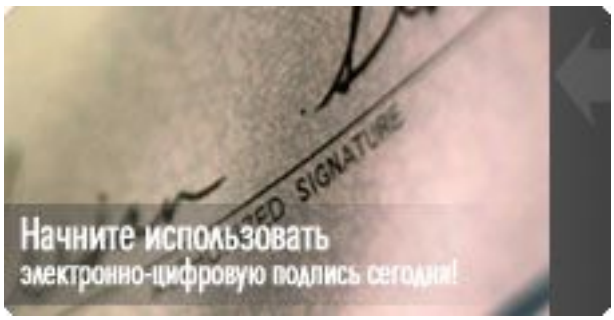
Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы.

Электронно-цифровая подпись.

Электронно-цифровые подписи обеспечивают защиту аутентификации и целостности электронных документов. Они могут использоваться при необходимости контроля с целью удостоверения, кто подписал электронный документ, а также при проверке, было ли содержание подписанного документа изменено. Рассмотрим подробнее нормативный документ об электронно-цифровой подписи. 10 января 2002 года Президентом был подписан закон «Об электронной цифровой подписи» номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года). Его роль поясняется в статье 1:

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.



2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия (Статья 3):

- ***Электронный документ*** - документ, в котором информация представлена в электронно-цифровой форме.
- ***Электронная цифровая подпись*** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
- ***Владелец сертификата ключа подписи*** - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- ***Средства электронной цифровой подписи*** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа

электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

- ***Сертификат средств электронной цифровой подписи*** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
- ***Закрытый ключ электронной цифровой подписи*** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- ***Открытый ключ электронной цифровой подписи*** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.
- ***Сертификат ключа подписи*** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.
- ***Подтверждение подлинности электронной цифровой подписи в электронном документе*** - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.
- ***Пользователь сертификата ключа подписи*** - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.
- ***Информационная система общего пользования*** - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.
- ***Корпоративная информационная система*** - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Согласно Закону, **электронная цифровая подпись в электронном документе равнозначна собственноручной подписи** в документе на бумажном носителе при одновременном соблюдении следующих **условий**:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет **сведения**, которые должен содержать **сертификат ключа подписи**:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Цифровые подписи могут применяться для любой формы документа, обрабатываемого электронным способом, например, при подписи электронных платежей, денежных переводов, контрактов и соглашений. Цифровые подписи могут быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой — для проверки подписи (открытый ключ). Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой имеющий к нему доступ может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Кроме того, очень важна защита целостности открытого ключа, которая обеспечивается при использовании сертификата открытого ключа

Следует уделять внимание выбору типа и качеству используемого алгоритма подписи и длине ключей. Необходимо, чтобы криптографические ключи, используемые для цифровых подписей, отличались от тех, которые используются для шифрования. При использовании цифровых подписей,

необходимо учитывать требования всех действующих законодательств, определяющих условия, при которых цифровая подпись имеет юридическую силу.

Может потребоваться наличие специальных контрактов или других соглашений, чтобы поддерживать использование цифровых подписей в случаях, когда законодательство в отношении цифровых подписей недостаточно развито. Необходимо воспользоваться консультацией юриста в отношении законов и нормативных актов, которые могут быть применимыми в отношении предполагаемого использовании организацией цифровых подписей.