Лекция 14

Вопросы информационной безопасности в Интернет.

Конфиденциальность — необходимость предотвращения разглашения какой-либо информации.

Согласно ФЗ «Об информации, информационных технологиях и защите информации», «*конфиденциальность информации* — ***обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя»***; а ***«****информация* — ***сведения (сообщения, данные) независимо от формы их представления»***.

- сведения о частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
- тайна следствия и судопроизводства;
- служебная тайна/государственная тайна;
- сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
- коммерческая тайна.

Закон «Об информации» разрешает обладателю информации наделять её статусом конфиденциальности самостоятельно.

Государственная тайна — защищаемые государством сведения, распространение которых может нанести ущерб безопасности Российской Федерации.

Коммерческая тайна — позволяет получить коммерческую выгоду — сведения производственные, технические, экономические, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

К.т. не могут быть сведения:
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической обстановке, безопасности пищевых продуктов...
- о численности, о составе работников, о системе оплаты труда...
- о задолженности работодателей по выплате заработной платы...
- о нарушениях законодательства...
- о размерах и структуре доходов некоммерческих организаций...

Основные меры по охране конфиденциальности информации:
- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, установление порядка обращения с этой информацией и контрольза соблюдением такого порядка;
- учёт лиц, получивших доступ к информации;
- регулирование отношений по использованию информации работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров

Конфиденциальность в Интернете — вопрос наиболее сложно регулируемый, так как сохранность данных зависит в основном от самого человека и от того, как, какую и в каком количестве информацию он предоставляет.

Аутентификация — процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им именем с паролем в базе данных пользователей или проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Авторизация — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.

Процедура идентификации напрямую связана с аутентификацией: субъект проходит процедуру аутентификации, и если аутентификация успешна, то информационная система на основе факторов аутентификации определяет идентификатор субъекта.

Например:
Идентификация пользователя:
факторы :: логин/пароль
идентификатор :: логин

Целостность информации — означает, что данные полны, т.е. условие того, что данные не были изменены при выполнении любой операции над ними.

Для проверки целостности данных широко используются хеш-функции MD5 и SHA. Такая функция преобразует совокупность данных в последовательность чисел. Если данные изменятся, то и последовательность чисел, генерируемая хеш-функцией тоже изменится.

Способы аутентификации:

- пароль многоразовый (хранение, передача, соль)
- пароль одноразовый:

- генератор паролей (ПСП или от времени)
- база паролей
- дополнительные пароли

- биометрическая:

- отпечатки пальцев (10^{-5} %)
- геометрия руки (2 %)
- радужная оболочка глаза (1 из 10^{78})
- распознавание по лицу (3 %)
- голос (5 %)
- подпись

- GPS
- многофакторная аутентификация