Чеченский государственный педагогический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Лекция № 2

Основные составляющие информационной безопасности. Понятие «информационная безопасность». Проблема информационной безопасности общества.

Лектор – Иноркаев Вахид Абу-Рашидович,
Старший преподаватель кафедры «Прикладная информатика (в экономике)»

Основные понятия информационной безопасности.

- **Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»**
- **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»**
- **Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**
- **Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»**
- **Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»**

Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

- **Защита информации** – группа методик правового, физического, технического, криптографического характера, нацеленных на противодействие информационным утечкам, несанкционированному доступу к данным, находящимся под защитой закона.
- **Информационные угрозы** – группа явлений, факторов, способных выступать в качестве вероятной или настоящей опасности, привести к нарушению безопасности данных.
- **Модель угроз** – совокупность представленных свойств, параметров возможных информационных угроз, выраженных в математическом, статистическом, физическом эквивалентах.
- **Уязвимость данных** – состояние информации или информационной системы, в ходе которого наблюдается вероятность реализации угроз.
- **Анализ информационных рисков** – совокупность количественных, качественных показателей, подтверждающих или прогнозирующих возможность реализации угроз в информационной системе и описывающих величины ущерба.

Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

- **Безопасность данных** – состояние, в ходе которого достигается поддержание таких свойств как конфиденциальность, целостность, доступность.
- **Цель защиты информации** – достижение недопущения возможного ущерба правообладателю данных, вызванного утечками, получением несанкционированного доступа к данным или случайными непреднамеренными действиями.
- **Средства защиты информации (СЗИ)** – комплекс программных, аппаратных решений, методов, подходящих для поддержания безопасности информации.
- **Способы защиты информации** – последовательность правил, рекомендаций, принципов при работе с данными и совокупность СЗИ.
- **Система защиты информации** – комплекс объектов, исполнителей, защитных техник, решений, объединенных в единое целое и функционирующих на основе исполнения известных норм, правил, законов в области информационной безопасности.

Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

- **Правовая защита информации:** Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

- **Техническая защита информации; ТЗИ:** Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

- **Криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования.

- **Физическая защита информации:** Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

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

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

- **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;
- **Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

- **Персональные данные** – сведения произвольного характера, которые косвенно или прямо способны идентифицировать конкретного человека.
- **Персональные данные с правом свободного распространения** – сведения, к которым открыт неограниченный доступ со стороны владельца путем заключения согласия на обработку.
- **Оператор** – любой орган, физическое или юридическое лицо, которые используют персональную информацию: обрабатывают, хранят, передают согласно установленным целям.
- **Обработка персональных данных** – процедура, в ходе которой происходит исполнение таких процессов как сбор, запись, систематизация информации вручную или посредством автоматизированных инструментов.

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

- **Автоматизированная система управления** - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;
- **Безопасность критической информационной инфраструктуры** - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;
- **Значимый объект критической информационной инфраструктуры** - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;
- **Компьютерная атака** - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

- **Критическая информационная инфраструктура** - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

- **Объекты критической информационной инфраструктуры** - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;
- **Субъекты критической информационной инфраструктуры** - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

- **Коммерческая тайна** - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
- **Разглашение информации, составляющей коммерческую тайну** - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.