Лекция #6

Правовые основы информатики

Структура лекции

- Роль **информационной безопасности** и ее место в системе национальной безопасности страны
- Задачи информационной безопасности
- Угрозы информационной безопасности
- Системный подход к построению систем защиты информации
- Средства защиты информации
- Информационная свобода
- Информационная война и виды информационного оружия
- Информационный терроризм

Введение

Общее понятие **«безопасность»**, широко употребляемое в русском языке, характеризует собой «положение, при котором не угрожает опасность кому-нибудь и чему-нибудь».

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».

Однако **«защита», «защищенность»** — это только одна сторона значения слова безопасность. С другой стороны, безопасность означает **отсутствие угрозы** со стороны объекта, явления или процесса, о безопасности которого идет речь, его безвредность. В связи с этим, когда мы говорим о безопасности чего-либо или кого-либо, необходимо рассматривать два плана:

внутренний — состояние защищенности от внешних угроз

внешний — безвредность для окружающих

Стратегия национальной безопасности

Понятия безопасности законодатель привел в **ст. 1 Закона о безопасности**, где безопасность определяется как **«состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».**

В **Стратегии национальной безопасности РФ** существенно дополнены и конкретизированы положения, ранее закрепленные в Законе о безопасности.

В Стратегии введено понятие **национальных интересов** как объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития.

При этом ограничен перечень областей, национальные интересы в которых определяют предмет национальной безопасности: **государственная, общественная, информационная, экологическая, экономическая, транспортная, энергетическая безопасность, безопасность личности.**

Национальные интересы

- ***Интересы личности*** определены в Концепции как полное обеспечение конституционных прав и свобод, личной безопасности, повышение качества и уровня жизни, физическое, духовное и интеллектуальное развитие.
- ***Интересы общества*** установлены в упрочении демократии, создании правового государства, достижении и поддержании общественного согласия, духовном обновлении России.
- ***Интересы государства*** состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии международного сотрудничества.

Роль информационной безопасности

Таким образом, укрепление **информационной безопасности** названо в Стратегии национальной безопасности РФ в числе важнейших долгосрочных задач.

Роль **информационной безопасности** и ее место в системе национальной безопасности страны определяется также тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое.

Доктрина информационной безопасности РФ

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации представлена в Доктрине информационной безопасности РФ.

В Доктрине информационной безопасности РФ **информационная безопасность** Российской Федерации определяется как:

состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются

- *реализация конституционных прав и свобод человека и гражданина,*
- *достойные качество и уровень жизни граждан,*
- *суверенитет,*
- *территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации,*
- *оборона и безопасность государства*

Информационная сфера общества

В научной литературе в составе **«информационной сферы общества»** выделяют:

- субъекты информационной сферы;
- общественные отношения в информационной сфере;
- информационную инфраструктуру общества;
- информацию.

Безопасность информации

Понятие **«безопасность информации»** распадается на две составляющие:

- **безопасность содержательной части (смысла)** информации— отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (например, информация, содержащаяся в программе для ЭВМ, именуемой компьютерным вирусом);
- **защищенность информации от внешних воздействий** - попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения.

Таким образом, защита информации входит составной частью в понятие безопасность информации.

Защита информации

Статьей 16 (ч. 1) **Закона об информации** устанавливается следующее.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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

Задачи информационной безопасности

Проблема ИБ включает, наряду с задачами обеспечения защищенности информации и информационных систем, еще два аспекта:

- защиту от воздействия *вредоносной* информации,
- обеспечение принятия обоснованных решений с *максимальным использованием доступной информации.*

Обеспечение ИБ призвано решать следующие основные **задачи**:

- выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам;
- защита прав юридических и физических лиц на интеллектуальную собственность, а также сбор, накопление и использование информации;
- защита государственной, служебной, коммерческой, личной и других видов тайны.

Угрозы информационной безопасности

Угрозы информационным системам и информационным ресурсам можно условно разделить на четыре основные группы:

- **программные** — внедрение «вирусов», аппаратных и программных закладок; уничтожение и модификация данных в информационных системах;
- **технические, в т.ч. радиоэлектронные**, — перехват информации в линиях связи; радиоэлектронное подавление сигнала в линиях связи и системах управления;
- **физические** — уничтожение средств обработки и носителей информации; хищение носителей, а также аппаратных или программных парольных ключей;
- **информационные** — нарушение регламентов информационного обмена; незаконные сбор и использование информации; несанкционированный доступ к информационным ресурсам; незаконное копирование данных в информационных системах; дезинформация, сокрытие или искажение информации; хищение информации из баз данных.

Системный подход

Противостоять этим угрозам можно на основе создания и внедрения эффективных систем защиты информации. Причем решение задачи создания таких систем должно быть реализовано на основе системного подхода по следующим причинам:

Во-первых, для эффективной защиты информационных ресурсов требуется реализация целого ряда разнородных мер, которые можно разделить на три группы: юридические, организационно-экономические и технологические.

Во-вторых, разработкой мер защиты применительно к каждой из трех групп должны заниматься специалисты из соответствующих областей знаний.

Системный подход

Меры по защите информационных ресурсов базируются на следующих принципах:

- нормативно-правовая база информационных отношений в обществе четко регламентирует механизмы обеспечения прав граждан свободно искать, получать, производить и распространять информацию любым законным способом;
- интересы обладателей информации охраняются законом;
- засекречивание (закрытие) информации является исключением из общего правила на доступ к информации;
- ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируются;
- специальной функцией государства является развитие сферы информационных услуг, оказываемых населению и специалистам на основе современных компьютерных сетей, системы общедоступных баз и банков данных, содержащих справочную информацию социально-экономического, культурного и бытового назначения, право доступа к которым гарантируется и регламентируется законодательством.

Системный подход

Применение в этих условиях системного подхода позволяет определить **взаимные связи** между соответствующими определениями, принципами, способами и механизмами защиты.

Причем понятие системности в данном случае заключается не просто в создании соответствующих механизмов защиты, а представляет собой **регулярный процесс**, осуществляемый на всех этапах жизненного цикла информационной системы.

Системный подход

Системный подход к защите информации требует, чтобы средства и действия, используемые для обеспечения информационной безопасности — *правовые*, *организационные, физические и программно-технические* — рассматривались как единый комплекс взаимосвязанных взаимодополняющих и взаимодействующих мер.

Один из основных принципов системного подхода к защите информации — **принцип «разумной достаточности»**, суть которого: *стопроцентной защиты не существует ни при каких обстоятельствах, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы.*

Право на доступ к информации

В последнее время формируется устойчивое мнение, что информация, существующая в форме знаний, должна быть общедоступна, потребность в ее получении у подавляющего большинства индивидов столь же велика, как и потребность в жизни или свободе.

И если право жизнь как первичное, фундаментальное ничем ограничить нельзя, ограничение права на свободу жестко регламентируется законом, то не менее жестко ***необходимо определять условия, при которых может быть ограничено право человека в доступе к необходимой ему информации****.*

То субъективное право, на котором мы заостряем внимание, касается *права человека свободно искать и получать информацию.*

И лишь к отдельным категориям информации, точно определенным нормативными правовыми актами, доступ может быть временно ограничен.

Основанием в таком ограничении является **защита охраняемых законом интересов личности, общества и государства.**

Несанкционированный доступ

Несанкционированный доступ — чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Проблема несанкционированного доступа к информации обострилась и приобрела особую значимость в связи с развитием компьютерных сетей, прежде всего глобальной сети Интернет.

Для успешной защиты своей информации пользователь должен иметь абсолютно ясное представление о возможных *путях несанкционированного доступа.*

Основные типовые пути несанкционированного получения информации

- хищение носителей информации и производственных отходов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- использование недостатков операционных систем и языков программирования;
- использование программных закладок и программных блоков типа «троянский конь»;
- перехват электронных излучений;
- перехват акустических излучений;
- дистанционное фотографирование;
- применение подслушивающих устройств;
- злоумышленный вывод из строя механизмов защиты и т.д.

Вредоносные программы

ст. 273 **УК РФ** выделяет следующие вредоносные последствия воздействия компьютерных вирусов на информацию:

- уничтожение,
- блокирование,
- модификация,
- копирование.

Уничтожение информации

Под уничтожением компьютерной информации ее **стирание в памяти ЭВМ**, оговаривая при этом, что уничтожением информации не является

- переименование файла,
- автоматическое «вытеснение» старых версий файлов последними по времени.

Под уничтожением информации также следует понимать и разрушение смысловых связей в отрезке информации, в результате чего он превращается в хаотический набор символов, *если восстановление таких связей с помощью той же программы невозможно.*

Модификация информации

Под *модификацией* компьютерной информации понимается внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ и базы данных.

Надо полагать, что модификация подразумевает все же не полное лишение отрезка информации смысла, а целенаправленное изменение смысла, приводящее либо к ложным выводам, либо к неправильному функционированию программы, если отрезком информации является программа для ЭВМ.

Блокирование и копирование информации

- под ***блокированием*** компьютерной информации понимается искусственное затруднение доступа пользователей к ней, не связанное с ее уничтожением.

- под ***копированием*** компьютерной информации следует понимать повторное однозначное устойчивое запечатление отрезка информации на машинном или ином материальном носителе

Средства защиты информации

Для *защиты информации от несанкционированного доступа* применяются:

- правовое регулирование
- организационные мероприятия,
- технические средства,
- программные средства,
- криптография и стеганография

Организационные мероприятия

- пропускной режим;
- хранение носителей и устройств в сейфе (диски, флешки, монитор, клавиатура и т.д.);
- ограничение доступа лиц в компьютерные помещения и т.д.

Технические средства защиты информации

Технические средства включают в себя различные аппаратные способы защиты информации:

- фильтры, экраны на аппаратуру;
- ключ для блокировки клавиатуры;
- устройства аутентификации — для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т.д.;
- электронные ключи на микросхемах и т.д.

Программные средства защиты информации

Программные средства защиты информации создаются в результате разработки специального программного обеспечения, которое бы не позволяло постороннему человеку, не знакомому с этим видом защиты, получать информацию из системы.

Программные средства включают в себя:

- парольный доступ-задание полномочий пользователя;
- блокировка экрана и клавиатуры;
- использование средств парольной защиты BIOS на сам BIOS и на ПК в целом и т.д.

Программные средства защиты информации

Программные средства защиты информации создаются в результате разработки специального программного обеспечения, которое бы не позволяло постороннему человеку, не знакомому с этим видом защиты, получать информацию из системы.

Программные средства включают в себя:

- парольный доступ-задание полномочий пользователя;
- блокировка экрана и клавиатуры;
- использование средств парольной защиты BIOS на сам BIOS и на ПК в целом и т.д.

Механизмы безопасности компьютерных сетей

- *Шифрование* применяется для реализации служб засекречивания и используется в ряде других служб.
- *Механизмы контроля доступа* обеспечивают реализацию службы безопасности, осуществляют проверку полномочий объектов сети, т.е. программ и пользователей, на доступ к ресурсам сети.
- *Цифровая подпись* по своей сути призвана служить электронным аналогом ручной подписи, используемой на бумажных документах.

Механизмы контроля доступа

Механизмы контроля доступа делятся на две основные группы:

- аутентификация объектов, требующих ресурса, с последующей проверкой допустимости доступа, для которой используется специальная информационная база контроля доступа;
- использование меток безопасности, наличие у объекта соответствующего мандата дает право на доступ к ресурсу.

Какие вы знаете
методы аутентификации
?

Свобода массовой информации

В Российской Федерации в период 90-х гг. был предпринят ряд существенных мер, направленных на обеспечение свободы массовой информации, которые нашли отражение в:

- Законе о СМИ,
- Федеральном законе от 13 января 1995 г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».

Информационная свобода: Польза или вред для общества?

Интернет и ей подобные системы — это новая степень свободы для человека, степень *информационной свободы.*

Эта свобода поиска и общения одновременно вдохновляет и настораживает.

В чем заключаются положительные и отрицательные стороны информационной свободы

?

Информационные войны

Осознание значимости информации для жизни человечества на новом качественном уровне в целом и построение коммуникаций, основанных на компьютерных технологиях в частности, сделали актуальным формирование новой стратегии силового противоборства между государствами — **стратегии *информационных войн.***

Как вы понимаете понятие информационной войны

?

Видеоматериал

Определение информационной войны

«Не знаю, каким оружием будут сражаться в третьей мировой войне, но в четвертой в ход пойдут камни и дубинки»

Альберт Эйнштейн

Информационной война - особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств.

См. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России. Учебное пособие. Под ред. Прохожева А.А. — М.: Всероссийский научно-технический информационный центр.2000. С. 34.

Информационное оружие

Информационное оружие - специальные средства, технологии и информация, позволяющие осуществлять «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства [1]

Информационное оружие - открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере [2]

1. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России. Учебное пособие. Под ред. Прохожева А.А. — М.: Всероссийский научно-технический информационный центр. 2000. С. 34.
2. Расторгуев СЛ. Информационная война как целенаправленное информационное воздействие информационных систем // Информационное общество. М., 1997. № 1. С. 64,65.

Классификация информационного оружия

- **стратегическое** — совокупность информации, технологий и средств реализации технологий, способных нанести неприемлемый ущерб политическим, экономическим и военным интересам страны, а также структурам, образующим ее стратегический потенциал, в рамках стратегической операции вооруженных сил государства;
- **оперативное** — совокупность видов информационного оружия, способного обеспечить решение важных задач при проведении операции вооруженных сил на определенном театре военных действий;
- **тактическое** — совокупность видов информационного оружия, способного обеспечить решение важных задач в ходе боевых действий или боя.

Специфические способы ведения информационной войны

- **радиоэлектронная борьба** (электронное подавление), которая заключается в создании помех средствам связи противника и его радиолокационным средствам;
- **хакерская война**, суть которой сводится к организации атак на вычислительные системы и сети, осуществляемых специально обученными лицами — хакерами, которые в состоянии проникнуть через системы защиты компьютерной информации с целью добычи нужных сведений либо выведения из строя программного обеспечения;
- **кибернетическая война**, суть которой заключается не в ведении реальных боевых действий, наносящих ущерб противнику, а в создании моделей, имитирующих такие действия.

Информационный терроризм

Усложнение процессов информационного общения между людьми, автоматизация управления промышленными объектами, транспортом и энергетикой породили **новые возможности целенаправленного негативного воздействия**, которые могут осуществлять как недружественные государства, так и отдельные группировки преступной направленности либо отдельные лица. Реализацию такой возможности принято именовать ***информационным терроризмом.***

Вирус Stuxnet

Вирус Stuxnet нанес серьезный урон иранской ядерной программе. Используя уязвимости операционной системы и человеческий фактор, Stuxnet успешно поразил 1368 из 5000 центрифуг на заводе по обогащению урана в Натанзе, а также сорвал сроки запуска ядерной АЭС в Бушере.

Ущерб, нанесенный ядерным объектам Ирана, сопоставим с ущербом от атаки израильских ВВС.

Это первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens.

Вирус Stuxnet

Создание подобного проекта требует огромных интеллектуальных и финансовых инвестиций, а значит, под силу лишь структурам масштаба государственных.

О военных целях вируса говорит **Евгений Касперский**:

«Stuxnet не крадет деньги, не шлет спам и не ворует конфиденциальную информацию. Этот зловред создан, чтобы контролировать производственные процессы, в буквальном смысле управлять огромными производственными мощностями. В недалеком прошлом мы боролись с кибер-преступниками и интернет-хулиганами, теперь, боюсь, наступает время кибертерроризма, кибероружия и кибервойн»

Вирус Stuxnet (видео)

Заключение

Следовательно, необходимо сформировать такую организационно-правовую систему, которая смогла бы координировать развитие информационной инфраструктуры нашей страны в целях предотвращения либо максимальной локализации последствий информационной войны или отдельных эпизодов применения информационного оружия.