Раздел 1 Теория информационной безопасности

Тема №2
МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

ВОПРОСЫ

2.1 ИНФОРМАЦИОННАЯ ВОЙНА КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

2.2 МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

2.3 ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: -2011-253с. (60 экз.Гриф УМО)

2.Расторгуев С.П. Основы информационной безопасности. .- М.: Издательский центр «Академия», 2008.- 192с. (20экз. Гриф УМО)

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» (ПСС Гарант, Интернет)

3. **Цифровая или кибервойна как реальность. Армейский вестник. 12 (дек.).2013г.**

2.1 Информационная война как угроза национальной безопасности

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ ОСОБЕННОСТИ

Термин «информационная война» (далее – ИВ) появился в середине 80-х г.г. в связи с новыми задачами Вооруженных Сил США после окончания «холодной войны». Начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г., когда новые информационные технологии впервые были использованы как средства ведения войны.

Под **информационной войной** понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии, посредством воздействия на информацию и ИС противника при одновременном обеспечении безопасности и защиты собственной информации и ИС. **(Понятие сформированное в военных кругах США)**

«информационная война» - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны; (Российская конвенция международной информационной безопасности).

Особенности информационной войны:

1. Охватывает **в качестве самостоятельных объектов все виды информации и информационных систем, отделяя информацию от среды использования;**

2. Объекты **могут выступать и как оружие, и как объект защиты;**

3. Расширяет **территорию и пространство ведения (традиционной войны), ведется как при объявлении войны, так и в кризисных ситуациях в различных сферах жизнедеятельности.**

4. Ведется как специализированными военными, так и гражданскими структурами.

2.1 Информационная война как угроза национальной безопасности

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ РАЗНОВИДНОСТИ

ВИДЫ ИВ

Информационно-психологическая война

Процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону.

ОБЪЕКТЫ ВОЗДЕЙСТВИЯ:

ЛЮДИ

Термин «информационно-психологическая война» был заимствован в русский язык из словаря военных кругов США. Перевод этого термина («information and psychological warfare») с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война», в зависимости от контекста конкретного официального документа или научной публикации[1].

Информационно- кибернетическая война

Кибервойна (англ. *Cyberwarfare*) — **противостояние в киберпространстве, в том числе компьютерное противостояние в Интернете, одна из разновидностей информационной войны.**

ОБЪЕКТЫ ВОЗДЕЙСТВИЯ:
ИС, ИТКС, АСУ ТП КВО ИИ (КСИИ), мобильные устройства, ИТ

2.1 Информационная война как угроза национальной безопасности

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ РАЗНОВИДНОСТИ

Информационно-психологическая война

ИПВ войны – это контентные войны, имеющие своей целью изменение массового, группового и индивидуального сознания. В процессе информационных войн идет борьба за умы, ценности, установки, поведенческие паттерны и т.п. Информационные войны велись задолго до интернета, насчитывают историю, измеряемую даже не сотнями, а тысячами лет. Интернет просто перевел эти войны на качественно иной уровень интенсивности, масштабности и эффективности.

ИПВ война ведётся между человеческими общностями, имеющими собственные системы власти, обладающими разными, в чём-то взаимоисключающими, антагонистическими системами ценностей, включающими идеологию и систему власти. Такими общностями являются признанные и непризнанные государства, союзы государств, стороны гражданской войны, экстремистские, в том числе террористические организации, стремящиеся к насильственному захвату власти, сепаратистские, освободительные движения.

Как правило, методами ИПВ являются вброс дезинформации или представление информации в выгодном для себя ключе. Данные методы позволяют изменять оценку происходящего населением территории противника, развивать пораженческое настроение, и, в перспективе, обеспечить переход на сторону ведущего информационное воздействие.. С появлением средств массовой информации и общим повышением уровня грамотности в XX веке ведение информационной войны стало более эффективным. Кроме традиционных средств массовой информации, в настоящее время эффективным инструментом информационной войны являются соцсети, что особенно ярко проявилось в ходе так называемой «арабской весны», Украинского «Майдана», ИПВ развязанной против России в связи с присоединением Крыма.

2.1 Информационная война как угроза национальной безопасности

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ РАЗНОВИДНОСТИ

Информационно-кибернетическая война

Термин

Термин «кибервойны» прочно вошел не только в лексикон военных и специалистов по информационной безопасности, но и политиков, представителей экспертного сообщества. Он стал одним из мемов, активно поддерживаемых и распространяемых СМИ всех форматов. Более того, кибервойны стали одной из наиболее обсуждаемых тем в социальных сетях, на интернет-площадках и т.п.

Понятие расширенное

По де-факто сложившемуся, но юридически не закрепленному, мнению подавляющего большинства военных и специалистов по информационной безопасности (вне зависимости от их страновой принадлежности) **под кибервойнами понимаются целенаправленные действия по причинению ущерба, перехвату управления или разрушению критически важных для функционирования общества и государства сетей и объектов, производственной, социальной, военной и финансовой инфраструктуры, а также роботизированных и высокоавтоматизированных производственных, технологических линий**.

История

Первое задокументированное использование кибероружия в ходе крупномасштабных военных действий связано с применением программ, блокирующих работу сирийских ПВО и радиоэлектронной разведки во время проведения так называемой операции «Оливы» в 2008 г.

Масштабное применение кибероружия впервые имело место по данным «Лаборатории Касперского» в Иране в 2010 г. В отличие от обычных вредоносных программ, работающих в популярных операционных системах, примененный против Ирана вирус Stuxnet был специально создан для проникновения в автоматизированные системы, регулирующие и управляющие определенным типом оборудования, связанным с конкретными технологическими цепочками в атомной промышленности. Как выяснилось позже он был создан в системе АНБ с участием израильских компаний для противодействия иранской атомной программе. Еще более сложная, многокомпонентная боевая программа была применена американцами и израильтянами против нефтяных терминалов и нефтеперерабатывающих заводов все того же Ирана.
Кроме того, были зафиксированы случаи использования компьютерных вирусов для вывода из строя систем SCADA крупнейшей саудовской нефтяной и катарской газовых компаний.

2.1 Информационная война как угроза национальной безопасности

Информационно-кибернетическая война

Силы информационно-кибернетической войны России

Войска информационных операций — формирование вооружённых сил РФ — России, находящееся в подчинении Министерства обороны РФ (Минобороны России).

Основными задачами являются централизованное проведение операций кибервойны, управление и защита военных компьютерных сети России, защита российских военных систем управления и связи от кибертерроризма и надежное закрытие проходящей в них информации от вероятного противника. Войска осуществляют координацию и интеграцию операций, проводимых киберподразделениями ВС России, экспертизу кибернетического потенциала Минобороны России и расширяют возможности его действий в кибернетическом пространстве.

В 2014 году создано Кибернетическое командование, основная задача которого заключается в защите от несанкционированного вмешательства в электронные системы управления России.

Силы информационно-кибернетической войны США

Первым специальным подразделением Вооружённых сил США, предназначенным для операций в киберпространстве, стало экспериментальное оперативное командование по отражению кибернетических угроз, созданное на базе 688-го крыла радиоэлектронной разведки ВВС в 2007 году. **Киберкомандование США начало функционировать 21 мая 2010 год**а,. Оно объединило под своим началом несколько ранее существовавших организаций, в частности, Соединение глобальных сетевых операций (англ.) и Объединённое командование сетевой войны (англ.). Агентство военных информационных систем (англ.) Военно-кибернетические операции США являются частью национальной стратегии безопасности киберпространства[. Новая военная стратегия США явно указывает, что кибератака на США является актом обычной войны[

2.1 Информационная война как угроза национальной безопасности

Информационно-кибернетическая война

ОСОБЕННОСТИ

1. Высокий уровень анонимности кибервойн. Он связан с трудностями дистрибуции киберагрессора. Частично эти трудности сопряжены с самой природой кибервойны, как воздействий в системе компьютер/компьютер через многослойные и запутанные сети электронных коммуникаций.

2. Неопределенность времени их начала. Все привычные человечеству виды войн начинались с хорошо фиксируемых материальных действий и соответственно имели четкую временную привязку. Многокомпонентные программы, как основное оружие кибервойн, могут проникать в сети и управляющие системы разнообразных военных и гражданских объектов и инфраструктур, заблаговременно.

3. Потенциальная бесследность. Любое известное вооружение имеет ярко выраженные признаки применения, которые позволяют с уверенностью говорить о начале, ходе и последствий военных действий.

4.Чрезвычайная сложность контроля кибервооружений со стороны государственных систем разведки и безопасности. Как признают многие специалисты, в наиболее изощренных вариантах по своим последствиям кибероружие сравнимо с применением ядерных боевых зарядов.

5.Чрезвычайная сложность контроля кибервооружений со стороны государственных систем разведки и безопасности. Как признают многие специалисты, в наиболее изощренных вариантах по своим последствиям кибероружие сравнимо с применением ядерных боевых зарядов.

6. Отсутствие для ИКВ каких-либо рамок международного регулирования. Как правило, отсутствие правового регулирования кибервойн связывают с непроработанностью юридических аспектов вследствие новизны вопроса. Однако, на наш взгляд, проблема гораздо глубже и серьезнее. На сегодняшний день интернет управляется организацией ICANN, фактически подконтрольной США и ее ближайшим союзникам. Важно, что регулирование осуществляется в рамках парадигмы «один мир – один интернет». При таком подходе вообще невозможны какие-либо привычные в военном праве межгосударственные соглашения. Дело в том, что ICANN отрицает право государств так или иначе регулировать, а значит, и нести ответственность за тот или иной сегмент интернета.

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ ОСОБЕННОСТИ

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ ПО ОЦЕНКАМ РОССИЙСКИХ СПЕЦСЛУЖБ, (ПРЕДУСМАТРИВАЕТ):

1. Подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);

2. Радиоэлектронная борьба (электромагнитное воздействие на элементы ИС и ИТКС, системы связи)

3. Радиоэлектронная разведка (получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специально внедренных в помещения и технические средства электронных устройств перехвата информации).

4 «Хакерная (кибернетическая) война» (осуществление НСД к ИР путем использования программно-аппаратных средств прорыва систем защиты ИС и ИТКС противника, с последующим их искажением, уничтожением или хищением либо нарушением нормального функционирования этих систем).

5. Психологическая война (формирование и массовое распространение по информационным каналам противника или глобальным сетям информационного взаимодействия дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения).

6. Получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в ИС, а также публикуемой в СМИ.

2.1 Информационная война как угроза национальной безопасности

ИНФОРМАЦИОННОЕ ОРУЖИЕ

ИНФОРМАЦИОННОЕ ОРУЖИЕ – это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всех средств высокотехнологичного обеспечения жизни общества и функционирования государства**.(Российскими экспертами и учёными) «информационное оружие»** - информационные технологии, средства и методы, предназначенные для ведения информационной войны; (Конвенция)

Информационное оружие от обычных средств поражения отличает:

1. Скрытность – возможность достигать цели без видимой подготовки и объявления войны;

2. Масштабность – возможность наносить невосполнимый ущерб, не признавая национальных границ и суверенитетов, без привычного ограничения пространства во всех сферах жизнедеятельности человека;

3.Универсальность – возможность многовариантного использования как военными, так и гражданскими структурами страны нападения против военных и гражданских объектов страны поражения.

Основные объекты применения ИО (как в мирное, так и в военное время) :

1. Компьютерные системы и системы связи, используемые государственными организациями при выполнении своих управленческих функций;
2. Военная информационная инфраструктура, решающая задачи управления войсками и боевыми средствами, сбора и обработки информации в интересах вооруженных сил;
4. Информационные и управленческие структуры банков, транспортных и промышленных предприятий;
5. СМИ, в первую очередь электронные (радио, телевидение и т.д.).

2.1 Информационная война как угроза национальной безопасности

ИНФОРМАЦИОННОЕ ОРУЖИЕ

***Сфера применения ИО** (включает как военную, так и экономическую, банковскую, социальную и иные области потенциального использования в целях):*

1. Дезорганизации деятельности управленческих структур, транспортных потоков и средств коммуникации;

2. Блокирования деятельности отдельных предприятий и банков, а также базовых отраслей промышленности (путем нарушения многозвенных технологических связей и системы взаиморасчетов, проведения валютно-финансовых махинаций и т.п.);

3. Инициирования крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;

4. Массового распространения и внедрения в сознание людей определенных представлений, привычек и поведенческих стереотипов;

5. Вызова недовольства или паники среди населения, а также провоцирования деструктивных действий различных социальных групп.

С появлением новых информационных технологий и организацией международного информационного обмена на новом уровне информационная составляющая в стратегии обеспечения информационной безопасности, (по оценкам Совета Безопасности РФ, руководителей российских спецслужб и Минобороны России), **вышла на первый план.**

2.2 Место информационной безопасности в системе национальной безопасности

ПОНЯТИЕ И СОВРЕМЕННАЯ СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Необходимым условием нормального существования и развития каждого общества является защищенность от внешних и внутренних угроз, устойчивость к попыткам внешнего давления, способность как парировать такие попытки и нейтрализовать возникающие угрозы, так и обеспечивать такие внутренние и внешние условия существования страны, которые гарантируют возможность стабильного и всестороннего прогресса общества и его граждан. Для характеристики этого состояния используется понятие Национальной безопасности.

Основные нормативные правовые акты в области национальной безопасности России

Стратегия национальной безопасности РФ 2015 г (утверждена указом Президента РФ)

Федеральный закон «О безопасности» 2010 г.

Понятие национальной безопасности

Национальная безопасность РФ - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан РФ, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие РФ.

Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией и законодательством РФ, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности

Система обеспечения национальной безопасности - совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов.

2.2 Место информационной безопасности в системе национальной безопасности

Нормативно-методические документы в области информационной безопасности

Межведомственная комиссия Совета безопасности России по информационной безопасности

ФУНКЦИИ

1) подготовка предложений и рекомендаций СБ по гос политике в области ИБ

2) анализ информации о состоянии ИБ РФ и предложения СБ по совершенствованию деятельности госорганов в области ИБ

3) анализ состояния ИБ ИТКС КВО и рекомендации госорганам по их защищённости

4) участие в подготовке предложений и рекомендаций СБ по разработке проектов нормативных правовых актов по ИБ РФ

5) другие

Доктрина информационной безопасности РФ (2000г., проект)

Стратегия развития информационного общества в РФ (2008г.)

Основы государственной политики РФ в области международной информационной безопасности на период до 2020 года (2013г.)

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ (2012 г.)

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
(2014 г.)

2.2 Место информационной безопасности в системе национальной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ

Место ИБ в системе НБ определяется важностью объектов обеспечения ИБ, угроз объектам ИБ и её влиянием на состояние национальной безопасности.

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ, поскольку объекты ИБ находятся во всех сферах жизнедеятельности.

Национальная безопасность РФ существенным образом зависит от обеспечения ИБ, и в ходе технического прогресса эта зависимость будет возрастать.

Наиболее важными мерами являются:

1. **Создание Межведомственной комиссии Совета Безопасности РФ по ИБ (1997г) и подкомитета в комитетете по безопасности Госдумы;**
2. **Разработка и принятие Доктрины информационной безопасности РФ (2000г);**
3. **Создание (1995г.,). и совершенствование системы подготовки кадров в области ИБ**
4. **Создание системы защиты государственной тайны, системы ПДТР и ТЗИ и других систем;**
5. **Разработка концепции правового обеспечения информационной безопасности.**
6. **Разработка и реализация мер по противодействию информационному оружию и информационной войне.**

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ СОДЕРЖИТ

Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина информационной безопасности РФ принята в 2000 году и утверждена Президентом РФ.

Доктрина ИБ РФ содержит

- Национальные интересы РФ в информационной сфере, виды и источники угроз ИБ РФ
- Методы обеспечения информационной безопасности
- Основные положения государственной политики
- Организационную основу и функции системы обеспечения ИБ РФ

2.3 Значение информационной безопасности для субъектов информационных отношений

ИНФОРМАЦИОННЫЕ ПРАВООТНОШЕНИЯ

Информационные отношения – это отношения, возникающие между субъектами в информационной сфере. Информационные отношения, регулируемые правом – информационные правоотношения. Нормы права, регулирующие информационные правоотношения содержаться в Федеральных законах России, основным из которых является Федеральный закон «Об информации, информационных технологиях и о защите информации».

Правоотношение - **обусловленное правовой нормой отношение между субъектами, которые имеют субъективные права и юридические обязанности.**

Структура информационного правоотношения

субъекты - носители права и обязанностей	**субъективные права и юридические обязанности**, определяющие содержание правоотношения	**объекты права**
Обладатели информации - гражданин (физическое лицо), - юридическое лицо, - Российская Федерация, - субъект РФ, -муниципальное образование. От имени РФ, субъекта РФ, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления	**Субъективные права** определяют возможность субъекта права действовать дозволенным образом и требовать определенного поведения от других субъектов (лиц) в связи с реализацией данного права. **Юридические обязанности** однозначны по их содержанию, императивны, непререкаемы, обеспечены юридическими механизмами, а также правом требования со стороны другого лица исполнения обязанности (право притязания).	- Информация - Информационные ресурсы - Информационные технологии (ИТ) - Информационные системы (ИС) - Информационно-телекоммуникационные сети (ИТКС) - другие

Информационные отношения – это отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.

2.3 Значение информационной безопасности для субъектов информационных отношений

ЗНАЧЕНИЕ ИБ ДЛЯ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Значение информационной безопасности для субъектов информационных отношений связано с <u>реализацией их прав и выполнения обязанностей</u> в рамках информационных правоотношений:

С правами:

1) с правом собственности на ИР, ИТ, ИС, ИТКС, включением их в состав имущества и использованием в качестве товара (в соответствии с Гражданским кодексом РФ);

2) с правом (информационными правами определёнными в Конституции РФ и информационном законодательстве):

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
2) использовать информацию, в том числе распространять ее, по своему усмотрению;
3) передавать информацию другим лицам по договору или на ином установленном законом основании;
4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

3) с реализацией права на доступ к информации;

С обязанностями

1) с выполнением обязанностей при осуществлении своих информационных прав:

1) соблюдать права и законные интересы иных субъектов права (лиц);
2) принимать меры по защите информации;
3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

2) с соблюдением конфиденциальности информации ограниченного доступа;

3) с обеспечением защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

2.3 Значение информационной безопасности для субъектов информационных отношений

ОСОБЕННОСТИ ПРАВ СОБСТВЕННОСТИ НА ИНФОРМАЦИЮ (ИР)

Отношения по поводу права собственности на ИР регулируются гражданским законодательством РФ, и имеют ряд особенностей:

1. ИР являются объектами отношений физических, юридических лиц, государства, составляют ИР России и защищаются законом наряду с другими ресурсами.
2. ИР могут быть товаром, за исключением случаев, предусмотренных законодательством РФ.
3. Право собственности на средства обработки информации не создает права собственности на ИР, принадлежащие другим собственникам.
4. ИР, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством РФ.
5. ИР, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.
6. ИР могут быть и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений.
7. На ИР распространяется право интеллектуальной собственности.
7. На ИС, ИТ, ИТКС распространяются право «вещной» собственности – имущественные права, а на содержащиеся в их составе объекты интеллектуальной собственности – право интеллектуальной собственности в т.ч. авторские права..

2.3 Значение информационной безопасности для субъектов информационных отношений

1. Информационные технологии –
процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных Федеральным законом «Об информации... .»;

2) развитие ИС различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в РФ ИТКС, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

2. Информационная система –
совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Право собственности на информационные системы принадлежит субъекту решением и на средства которого они созданы.

1) государственные ИС (федеральные и региональные - собственник государство)

2) **муниципальные ИС**, созданные на основании решения органа местного самоуправления (собственники - муниципальные органы);

3) **иные информационные системы** (собственники юридические и физические лица).

Субъекты, осуществляющие эксплуатацию ИС, являются операторами.

2.3 Значение информационной безопасности для субъектов информационных отношений

3. Информационно-телекоммуникационная сеть
- технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием СВТ

Использование информационно-телекоммуникационных сетей

1. На территории РФ использование ИТКС осуществляется с соблюдением требований законодательства РФ в области связи, Федерального закона «Об информации ..» и иных нормативных правовых актов РФ.

2. Регулирование использования ИТКС, доступ к которым не ограничен определенным кругом лиц, осуществляется в РФ с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области (Интернет). Порядок использования иных ИТКС определяется владельцами таких сетей с учетом требований, установленных Федеральным законом «Об информации».

3. Использование ИТКС в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений этой деятельности.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности.

5. Передача информации посредством использования ИТКС осуществляется без ограничений. Ограничения могут быть установлены только законом.

6. Особенности подключения государственных ИС к ИТКС могут быть установлены нормативным правовым актом Президента или Правительства РФ.

ЗАДАНИЕ НА СРС

1. Ознакомиться со стратегией национальной безопасности (ПСС Гарант, Интернет).
2. Ознакомиться с Федеральным законом «Об информации, информационных технологиях и о защите информации» 2006г.
3. Выписать в тетрадь объекты и субъекты информационных правоотношений.
4. Выписать в тетрадь понятия ИР, ИТ, ИС, ИТКС.
5. Подготовиться по вопросам семинара.

СЕМИНАР №2
МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Вопросы семинара

1. Информационная война как угроза национальной безопасности. Понятие информационной войны и её особенности. Концепция информационной войны по оценкам Российских спецслужб. Информационное оружие: понятие, отличие от обычных средств поражения, объекты применения. Сфера применения информационного оружия.

2. Место информационной безопасности в системе национальной безопасности России. Понятие и современная стратегия национальной безопасности России. Информационная безопасность в системе национальной безопасности РФ. Наиболее важные меры, характеризующие важность информационной безопасности для национальной безопасности.

3. Значение информационной безопасности для субъектов информационных отношений. Понятие и структура информационного правоотношения. Состав информационных правоотношений. Значение ИБ для субъектов информационных отношений, связанное с их правами. Значение ИБ для субъектов информационных отношений, связанное с их обязанностями.

1. Доклад: Информационная война и информационное оружие.

Литература

1. Методические рекомендации к курсу.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» 2006г. (ПСС Гарант, Интернет)
3. Стратегия национальной безопасности РФ до 2020 года. (ПСС Гарант, Интернет)