ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 63 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 63 кафедры
полковник_____С.Войцеховский

«___» _____ 2015 г.

Автор: преподаватель 63 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 1

Тема: «ВВЕДЕНИЕ. СУЩНОСТЬ ЗАЩИТЫ ИПО»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 63 кафедры
протокол № _ от «____» _____ 2015 г.

Санкт-Петербург
2015

Содержание занятия и время

Введение – 5-7 мин.

Учебные вопросы (основная часть):

1. Предмет, цель и задачи дисциплины. Порядок изучения дисциплины. Литература. – 20 мин.
2. Содержание предметной области защиты информации – 30 мин.
3. Сущность и цели защиты ИПО – 20 мин.
4. Основные положения доктрины информационной безопасности РФ – 10 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.
3. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.:СОЛОН-Пресс, 2002. – 272 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Ознакомиться с предметом дисциплины, приобрести знания о предметной области защиты информации.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на необходимости ЗИ в ВС РФ, порядке изучения дисциплины, предметной области ЗИ.

В заключительной части обобщить изложенный материал и сформулировать задание на самостоятельную подготовку, осуществить контрольный опрос.

1. Что является предметом учебной дисциплины?
2. Что такое защита информации?
3. На какие составляющие подразделяется предметная область ЗИ?

Товарищи курсанты! Я майор Краснов Сергей Александрович – старший преподаватель 63 кафедры. В течение этого семестра я буду проводить у вас лекционные и практические занятия по дисциплине **«ЗАЩИТА ИНФОРМАЦИИ»**, к изучению которой мы сегодня с вами приступаем.

Вступление.

В настоящее время во всём мире, в том числе и России, широко обсуждаются проблемы создания глобального информационного общества (ГИО), характеризующегося постоянным ростом объёмов информации и огромным информационным обменом. Создание ГИО в России -– часть национальной стратегии перехода к ускоренному экономическому развитию. Одним из основных критериев развития такого общества является качество и уровень внедрения компьютерных информационно-телекоммуникационных технологий (ИТТ), где важнейшим компонентом является информационная безопасность (ИБ). Внимание к ИБ обусловлено прежде всего тем, что параллельно с развитием и внедрением ИТТ, активно развиваются и находят практическое применение методы и средства атак на информационно-телекоммуникационные системы.

В последнее время в средствах массовой информации все чаще звучит термин «информационная война». Наступивший век называют не только веком информационных технологий, но и веком информационных конфликтов.

Информационная война – открытые или скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере. Информационные воздействия или информационные операции осуществляются с применением, как информационного оружия, так и других средств воздействия на информацию и информационные системы противника. К этим средствам можно отнести все виды физического воздействия, начиная от электромагнитного и заканчивая механическим разрушением носителей информации. (*Информационное оружие* – это средство воздействия на информацию информацией).

С конца 80-х годов по настоящее время против России ведется настоящая информационная война, итогами которой являются следующие признаки (Расторгуев С. П. Информационная война. - М: Радио и связь, 1998):

- гибель и эмиграция части населения (в первую очередь, научного человеческого потенциала);
- вывоз из страны наиболее перспективных наукоемких технологий;
- разрушение системы образования;
- разрушение промышленности;
- активная пропаганда чуждого образа жизни (как вид информационного воздействия);
- потеря части территорий;
- политическая зависимость от других стран, потеря собственных интересов и зон влияния;
- резкое сокращение, деморализация армии и пр.

Информационная война никем не объявляется, никогда не прекращается, ведётся с использованием самых современных программно-аппаратных средств, не знает границ в пространстве и времени. Её результаты становятся достоянием общественности в лучшем случае только спустя многие годы.

Так Томас Рид, одно время главком Военно-воздушных сил США, а затем член Совета национальной безопасности в администрации президента Рейгана, только в 1996 году в своей книге «История холодной войны глазами очевидца» (Insider's History of the Cold War» by Thomas Reed) рассказывает о неизвестных эпизодах великого противостояния между США и СССР происходивших в начале 80-х. В своих мемуарах он впервые поведал, что летом 1982 года в безлюдной части Сибири - произошел чудовищной силы взрыв - газопровода (около трех килотонн, в тротиловом эквиваленте). Причиной этого стало то, что в начале 1980-х годов США в нужный момент подсунули СССР, через третьи страны, программное обеспечение для

трубопроводов, управлявшее работой насосов, турбин и вентилей. Поставленная компьютерная система оказалась с «закладкой». По словам Рида, это было сделано с помощью преднамеренно испорченных микросхем и программного обеспечения. (Я бы сказал специально изготовленных микросхем и ПО). В нужный момент параметры программы внезапно начинали изменяться, порождая чрезмерное давление в трубах. В результате взрыв. Так американские спецслужбы пытались ставить палки в колеса советской экономике.

Директива Президента США «*Об управлении шифрованием в обществе» (Public Encryption Management*), однозначно устанавливает, что экспортируемые из США СКЗИ не должны служить препятствием для органов электронной разведки США при добывании ими необходимой информации в компьютерных сетях на территории любой страны земного шара. Другими словами, если какое-то СКЗИ было экспортировано из США, это однозначно свидетельствует о том, что соответствующим компетентным органам этой страны (и, скорее всего, не только этой) не составляет особого труда «взломать» данное средство.

Информационная безопасность России является частью ее национальной безопасности и должна выполнять следующие функции:

- обеспечивать ее «информационный суверенитет, т.е. формировать и проводить политику исходя из интересов национальной безопасности России;
- способствовать успешному проведению экономических преобразований, укреплению политической стабильности общества.

Решение этих задач возможно только при создании системы комплексной защиты информации и правильной организации ее функционирования. А это в свою очередь требует наличия высококвалифицированных специалистов.

В.1. Предмет, цель и задачи дисциплины. Порядок изучения дисциплины.

Предметом учебной дисциплины **«Защита информации»** являются принципы построения, организация применения эффективных средств и методов защиты информации на объектах ВТ войск ВКО.

Целью учебной дисциплины является формирование у курсантов знаний и практических навыков по организации защиты информации и использованию различных методов и средств защиты компьютерной информации на объектах ВТ, в автоматизированных системах и сетях.

Задача учебной дисциплины: подготовка курсантов к эффективному использованию современных методов и средств защиты компьютерной информации на объектах вычислительной техники войск ВКО.

Дисциплина базируется на учебном материале, изложенном в программах следующих дисциплин:

— высшая математика;
— информатика;
— операционные системы.

Дисциплина обеспечивает изучение таких дисциплин, как:

— криптография;
— защита информации в вычислительных комплексах и сетях,
— эксплуатация программного обеспечения.

Основными видами занятий при изучении дисциплины являются лекции, практические занятия, самостоятельные занятия под руководством преподавателя, а также занятия в часы самостоятельной подготовки.

Дисциплина несекретная
Изучается в 6 и 7 семестре.

Всего часов – 126
лекций – 40 ч.
практических занятий – 56 ч.
курсовое проектирование 14 ч.
групповые занятия 4 ч.
Контрольная работа 2 ч.
ср под рук. преп. – 4 ч.
Изучение дисциплины завершается экзаменом

ЛИТЕРАТУРА

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.
3. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.
4. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
5. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.
6. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.:СОЛОН-Пресс, 2002. – 272 с.
7. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000.- 450
8. Костромин В.А. Самоучитель Linux для пользователя. – СПб.: БХВ-Петербург, 2003. – 672 с.
9. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: МГТУ им. Н.Э. Баумана, 2002. –304 с.
10. Общесистемные вопросы защиты информации. Коллективная монография/ под ред. Е.М. Сухорева. Кн. 1 – М.: Радиотехника, 2003. – 296 с.
11. Основы современных компьютерных технологий: Учебник/ под ред. Проф. А.Д.Хомоненко – СПб.: КОРОНА принт, 2005. – 672 с.
12. Петренко С.А., Петренко А.А. Аудит безопасности INTRANET. – М.: ДМК Пресс, 2002. – 416 с.

Государственные стандарты РФ:

13.1 . ГОСТ Р 50922-96 Защита информации. Основные термины и определения. Дата введения 1.07.97 г.

13.2. ГОСТ РВ 51987-2002 Типовые требования и показатели качества функционирования информационных систем. Дата введения 1.07.2003г

13.3. ГОСТ Р 51275-1999 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

13.4. ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

13.5. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

Руководящие документы:

14.1. Доктрина информационной безопасности РФ.

14.2. Военная доктрина РФ.

14.3. ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ.

14.4. РД Вирусы – ФСТЭК, 2005 г.

14.5. Сборник РД ГТК – ФСТЭК, 2005.

Приказы Министра обороны:

15.1. Приказ Министра обороны Российской Федерации № 010 от 2005 г.
15.2. Приказ Министра обороны Российской Федерации № 011 от 2013 г.
15.3. Приказ МО РФ № 046.
15.4. Приказ Министра обороны Российской Федерации № 190 от 13.05.02 г. «О принятии на снабжение ВС РФ защищенных ОС МСВС 3.0, СУБД «Линтер-ВС» 6.0 и комплекса программных средств обеспечения повседневной деятельности должностных лиц КП «Офис» 1.0».
№ 392 МО РФ от 2004 г. «О мерах по обеспечению информационной безопасности в ВС РФ при использовании международных сетей (Интернет)».

Директива Генерального штаба ВС РФ: «Концепция развития системы управления ВС РФ на период до 2016 года», утверждена НШГ–1-м заместителем МО РФ 11.01.2002 г.

В.2. Содержание предметной области защиты информации.

Под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-96]. Данный вид деятельности образует сложную предметную область, включающую разнородные и разноуровневые составляющие, находящиеся во взаимосвязи друг с другом.

По видам деятельности **предметная область «ЗИ»** подразделяется на три составляющие:

1. собственно *процесс ЗИ* как совокупность действий по применению методов (способов) и средств ЗИ;
2. *управление ЗИ* как совокупность целенаправленных воздействий органов управления на объекты защиты, силы и средства ЗИ;
3. *обеспечение ЗИ*, под которым понимается создание необходимых образовательных, научных, технических, информационных и других условий для реализации процесса ЗИ.

1. *Процесс ЗИ* характеризуются тремя составляющими:

- объектами защиты;
- угрозами, от которых необходимо обеспечить защиту объектов;
- методами (способами) и средствами защиты объектов от угроз.

Объекты защиты определяется тремя составляющими:

- информацией;
- носителем защищаемой информации;
- информационным процессом, протекающим на носителе, или физическим процессом, в котором участвует носитель защищаемой информации.

Указанные выше составляющие описания объекта защиты взаимосвязаны. Только тогда, когда имеется защищаемая информация, представленная на ее носителе, и этот носитель участвует в некотором процессе, появляется потенциальная опасность утечки информации или воздействия на нее. Структура понятия «объект защиты» представлена на рис. 1.

Угроза безопасности информации представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Под методом (способом) ЗИ понимают порядок и правила применения соответствующих принципов и средств ЗИ.

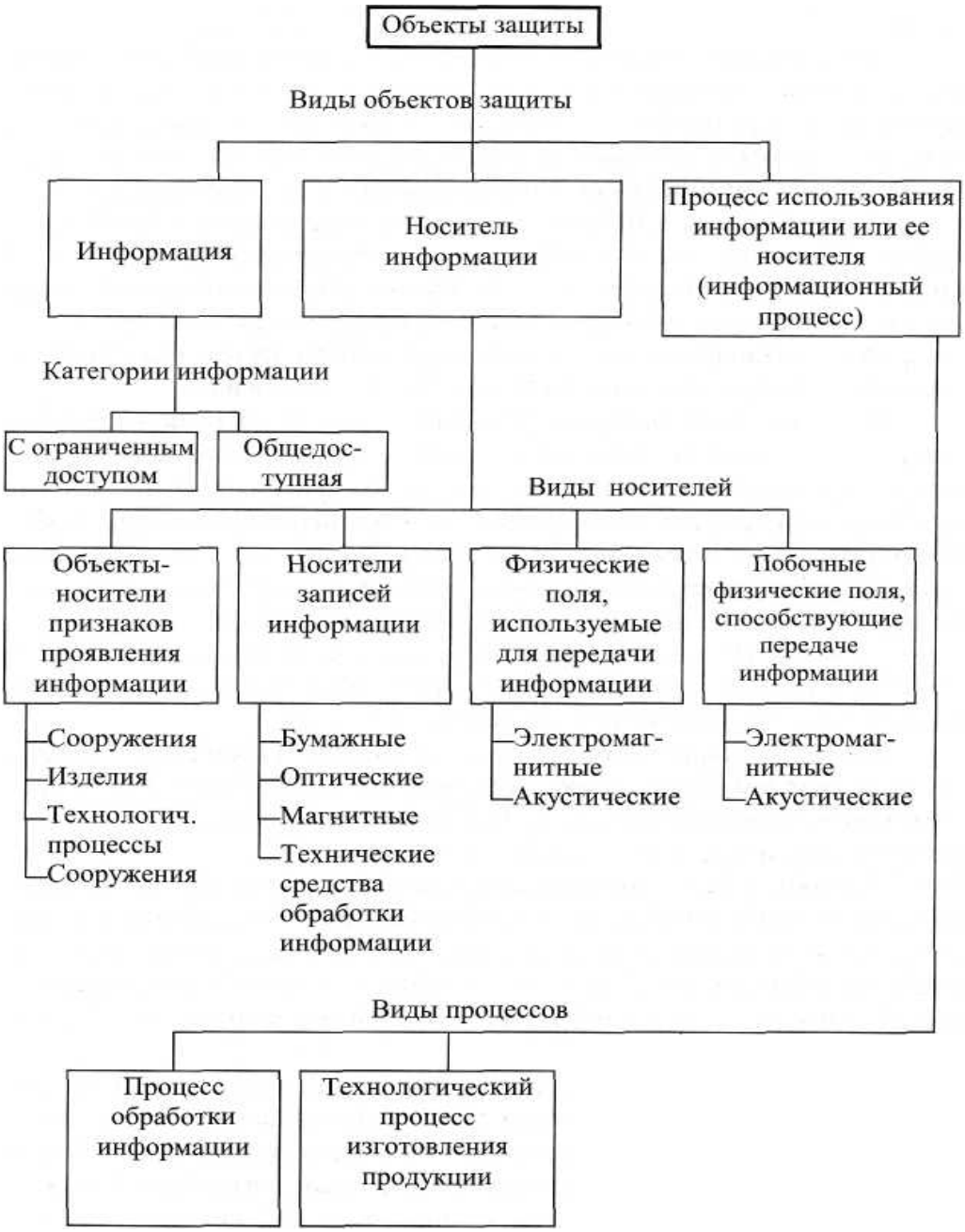


Рис. 1. Структурное представление понятия «объект защиты»

2. Управление ЗИ в зависимости от используемых методов и степени свободы объектов управления подразделяется на следующие виды:

- управление техническими средствами и системами ЗИ;
- директивное управление подчиненными органами ЗИ;
- координацию деятельности нескольких самостоятельных организационных структур системы ЗИ на основе согласования решений их органов управления;
- функциональное регулирование деятельности в области ЗИ, под которым понимается создание и обеспечение выполнения общих правил и норм в области ЗИ в интересах реализации единой технической политики в области ЗИ.

3. Обеспечение ЗИ включает в себя материально-техническое обеспечение деятельности органов и средств ЗИ, образовательную деятельность в области ЗИ, проведение НИОКР в области ЗИ, оказание услуг по ЗИ и др.

Процессы ЗИ, управление ЗИ и обеспечение ЗИ взаимосвязаны и выполняются организационно-технической системой ЗИ (ОТСЗИ). По своему построению ОТСЗИ могут быть

многоуровневыми и многофункциональными. В зависимости от масштаба решаемых задач ОТСЗИ могут образовывать иерархию, включающую следующие уровни:

- межгосударственные системы ЗИ (например, союзного государства);
- национальные системы ЗИ, включающие государственные и негосударственные компоненты;
- ведомственные (отраслевые) системы ЗИ федеральных органов исполнительной власти;
- региональные системы ЗИ в федеральных округах (ФО) Российской Федерации;
- системы ЗИ субъектов Российской Федерации;
- системы ЗИ предприятий, учреждений и организаций;
- системы ЗИ на конкретных объектах защиты.

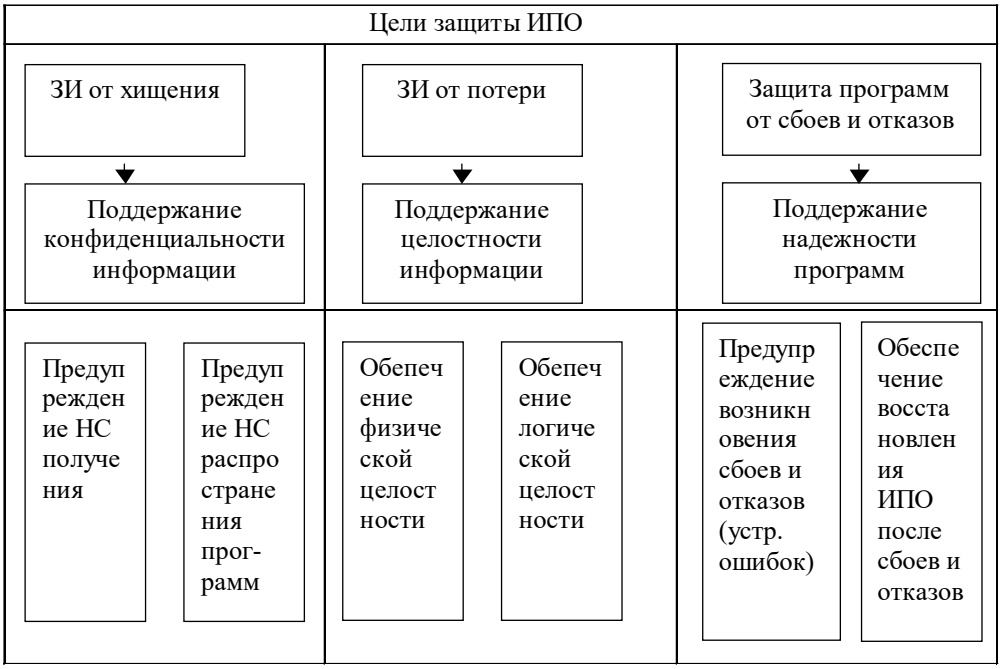
В.3. Сущность и цели защиты ИПО.

Защита ИПО – использование средств и методов, принятие мер и осуществление мероприятий с целью обеспечения безопасности хранимой и обрабатываемой информации, а также используемых в ВС программных средств.

Безопасность ИПО – это состояние информации, которое соответствует установленному статусу ее хранения и использования.

Понятие защиты имеет смысл, когда известны цели защиты, определяющие от чего надо защищать данные объекты.

Цели защиты ИПО можно представить в виде следующей схемы:



Целостность информации – способность обеспечивать ее неизменность (физическая целостность) и непротиворечивость (логическая целостность) в процессе хранения и обработки данных.

Конфиденциальность данных – доступность их только для тех лиц, которые имеют на это соответствующие полномочия. При этом необходимо обеспечить защиту не только данных от НС получения, но и защиту программ от несанкционированного распространения.

Надежность программных средств – способность точно и своевременно выполнять все свои функции. Для надежности обработки данных необходимо отсутствие ошибок в программных и аппаратных средствах ВС, что достигается в процессе разработки и сопровождения соответствующих компонентов. Следует учитывать, что полное отсутствие ошибок гарантировать невозможно. Следовательно для надежной работы должны быть предусмотрены возможности оперативного восстановления работоспособности программ после сбоев и отказов.

В. 4. Основные положения доктрины информационной безопасности РФ (утверждена президентом РФ 9 сентября 2000 г.)

(Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.)

4.1. Информационная безопасность РФ. Национальные интересы РФ в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

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

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, 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 и пользования информацией, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, развитии равноправного и взаимовыгодного международного сотрудничества.

В доктрине информационной безопасности Российской Федерации, утвержденной Президентом РФ 09.09.2000г., определены национальные интересы РФ в информационной сфере, которые объединены в три основные группы:

1. Национальные интересы, связанные с соблюдением конституционных прав граждан в области получения информации и пользования ею;
2. Национальные интересы, связанные с развитием современных отечественных телекоммуникационных технологий;
3. Национальные интересы, связанные с развитием государственных информационных ресурсов.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

В доктрине проанализированы угрозы внешнего и внутреннего характера национальным интересам РФ, защита от которых составляет основное содержание деятельности по обеспечению информационной безопасности. Можно утверждать, что приведенные в доктрине выводы об угрозах развитию отечественной индустрии средств информатизации, телекоммуникации и связи (эти выводы можно расширить и на другие области экономической и общественной деятельности), являются следствием уже примененной к России совокупности внешних воздействий информационного и экономического характера, а также внутренних причин.

Результатами этих воздействий можно считать следующие, приведенные в доктрине факторы:

- ограничение доступа Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации и информационных продуктов, а также противодействия усилению технологической независимости Российской Федерации от зарубежных стран в области информатизации;
- вытеснение с отечественного рынка средств информатизации, телекоммуникации и связи российских производителей;
- увеличение оттока квалифицированных кадров из России, их перехода в зарубежные компании;
- усиление зависимости духовной жизни общества, экономической и политической жизни страны от зарубежных информационных структур;
- снижение уровня образованности граждан, существенно осложняющего подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных.

4.2. Виды угроз информационной безопасности Российской Федерации

Перечисленные в доктрине угрозы информационной сфере государства, в соответствии с введенной выше классификацией направлений информационной безопасности, можно объединить в следующие группы.

1. *Угрозы несанкционированному, неправомерному доступу к информации и информационным системам.* К ним относятся угрозы:

- раскрытия сведений конфиденциального характера, а также другие, охраняемые законом сведения;
- ущемления законных интересов человека, связанных с использованием результатов его интеллектуальной деятельности;
- нарушения персоналом или посторонними лицами установленного регламента работы информационно - телекоммуникационных систем и сетей связи, нормального функционирования компонентов, нарушения принятой технологии обработки информации в этих системах и сетях, получения несанкционированного доступа к обрабатываемой в них информации, в том числе по техническим каналам связи;
- внедрения в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия, а также незаконного внедрения электронных устройств перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти и организаций;
- воздействия на парольно - ключевые системы защиты автоматизированных систем обработки и передачи информации, хищения ключей и средств криптографической защиты информации.

2. *Угрозы разрушению {утрате) информации и информационных систем.* К этой группе угроз можно отнести следующие:

- разрушение систем накопления и сохранения культурных ценностей, включая архивные фонды;
- уничтожения, повреждения, разрушения или хищения машинных и других носителей информации.

3. *Угрозы, связанные с явным и неявным воздействием посредством информации.*

В доктрине обозначены следующие угрозы:

- использования средств массовой информации для ограничения права человека на свободный выбор убеждений;

- пропаганды образцов массовой культуры, основанных на культе насилия, духовных и нравственных ценностях, противоречащих нормам, принятым в российском обществе;
- злоупотребления свободой массовой информации;
- противоправного применения органами государственной власти, общественными российскими и зарубежными организациями, спецслужбами иностранных государств, криминальными структурами специальных средств воздействия на индивидуальное, групповое и массовое сознание;
- перехвата, дешифрации и навязывания ложной информации в сетях передачи данных, линиях связи;
- разработки и распространения программ, нарушающих нормальное функционирование информационных и информационно - телекоммуникационных систем, в том числе систем защиты информации.

4.3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

1- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур;

2- стремление ряда стран к доминированию и ущемлению интересов России в мире;

3- обострение международной конкуренции за обладание информационными технологиями и ресурсами;

4- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

5- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

6- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

1- критическое состояние отечественных отраслей промышленности;

2- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур;

3- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере;

4- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

5- недостаточная экономическая мощь государства;

6- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

7- отставание России от ведущих стран мира по уровню информатизации.

4.4. Основные задачи по обеспечению информационной безопасности РФ

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных

информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

1- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;

2- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации;

3- включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации;

4- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;

5- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;

6- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации,;

7- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;

8- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

9- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

10- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

11- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

В. 5. «Доктрина информационных операций» США.

По поводу 2 пункта внешних угроз *«стремления ряда стран к доминированию и ущемлению интересов России в мире»*. В США, например, проблемам достижения превосходства в информационных конфликтах, проблемам сохранения национальных интересов в информационном противоборстве, стратегии и тактике применения информационного оружия в конфликтах на различных фазах их развития, судя по источникам информации, уделяется значительное внимание. Так, например, «**Доктрина информационных операций**», разработанная в **США** [*Завадский И .И.* Информационная война - что это такое? Защита информации. - Конфидент, 1996, №4], описывает основные принципы ведения информационной войны, как в условиях вооруженного конфликта, так и в мирный период противоборства двух и более организационных структур.

Вся совокупность информационных операций (ИО), применяемых конфликтующими сторонами, может быть условно разделена на наступательные и оборонительные, причем и те и другие планируются и реализуются совместно и взаимоувязано.

Наступательные информационные операции включают интегрированное использование совокупности возможностей и действий, поддержанных разведанными сведениями и

направленных на достижение определенных целей. Другими словами, наступательная ИО представляет собой процесс моделирования поведения противника на основе полученных сведений о нем, модификации этой модели в соответствии с целями нападающей стороны и формировании у противника этой модифицированной модели путем воздействия на него специально подготовленными данными. Самым эффективным и быстро приносящим результаты воздействием считаются ИО, направленные на органы подготовки и принятия решения противника.

Основной принцип применения наступательных ИО, согласно разработанной в США доктрине, заключается в том, что основными объектами их воздействия являются процессы принятия решений человеком.

*К **наступательным** ИО можно отнести* также операции:

- психологические воздействия, например суггестия - скрытое информационное воздействие на организационно-техническую, социальную систему или отдельные личности, как правило, те, на которые возложены функции принятия решений;
- дезинформация;
- радиоэлектронная борьба, как средство воздействия на телекоммуникационные средства и специальные радиоэлектронные средства противоборствующей стороны;
- компьютерные сетевые атаки, в состав которых входят такие воздействия, как распространение компьютерных вирусов, нарушение систем контроля доступа в корпоративные информационные сети, сети банковских структур, информационные сети управленческих структур и пр.;
- физическая атака (разрушение) информации и информационных систем противника.

Наступательные ИО поддерживаются организационными мероприятиями и техническими средствами, обеспечивающими их секретность и скрытность. Их подготовка и проведение сопровождаются сбором информации о противоборствующей стороне и ее аналитическим исследованием. Таким образом, **разведка и шпионаж** можно отнести к разновидностям наступательных ИО. Одна из основных задач планирования и проведения наступательных ИО состоит в обеспечении их скрытности, невидимости для противника. **Коварность информационной агрессии** заключается в том, что она может проводиться вне явного проявления конфликта между противоборствующими сторонами. Сторона, против которой применяется информационное оружие, может и не подозревать об этом, и только при вхождении конфликта в активную фазу, наряду со скрытыми угрозами и операциями в ход идут явные информационные операции, такие как поражение телекоммуникационных средств противника постановкой помех, разрушение информационных систем путем активизации специально введенных в них программно-аппаратных средств и прочее.

К *неявным информационным операциям* относится, в первую очередь, психологическое воздействие. **Под психологической информационной операцией** (ПСИОП) понимают совокупность действий по передаче противнику выборочной информации и установок. Эти операции разрабатываются с целью оказания влияния на эмоции, мотивации, отношения, доминанты, рассуждения, логические выводы и, в конечном счете, на поведение управленческих структур и организаций противника, отдельных групп населения и отдельные личности противоборствующей стороны. Они имеют стратегические, операционные и тактические прикладные программы, включая информационные воздействия, осуществляющие военный обман и дезинформацию противника.

В стратегическом плане ПСИОП могут принимать форму политических или дипломатических действий, объявлений или сообщений. На операционном плане ПСИОП может включать распространение листовок, передачу сообщений с помощью радио и телевизионных широковещательных передач и другие способы передачи информации, которые направлены на деморализацию, бездействие, отступление или сдачу вражеских сил. Постоянное осуществление ПСИОП ускоряет деморализацию противника и способствует дезертирству. На тактическом уровне ПСИОП включает различные способы воздействия, направленные на поддержание постоянного страха и разногласия во вражеских рядах; ПСИОП может влиять на поведение отдельных личностей через непосредственную связь с ними.

Доктрина информационных операций США рассматривает, в частности, операции оказания **гуманитарной помощи** как разновидность информационного воздействия. Примером прекрасно спланированной и успешно реализованной информационной операции может служить создание США фондов поддержки развивающихся стран, через которые осуществлялась финансовая поддержка ученых и развитие в этих странах телекоммуникационных сетей и Интернет-технологий. Цели этой операции - психологическое воздействие на слои общества, являющиеся носителями передовых и критических технологий, создание условий для их эмиграции в США и другие страны запада, создание и расширение технологической базы в виде Интернет для расширения информационной агрессии. В 1999 г. в США разработана архитектура и концепция военных операций через Интернет.

Другим примером применения ПСИОП служит **манипуляция сведениями о событиях**, происходящих в недружественной стране, и представление их в собственных СМИ в таком виде, чтобы сформировать в негативном плане мировое общественное мнение, осуществить ее информационную изоляцию, оправдать применение экономических санкций. Такая информационная операция проводится в настоящее время против России на основе манипуляции сведениями о событиях в Чечне.

Особой областью информационного противоборства являются **средства и методы ведения радиоэлектронной борьбы (РЭБ)**. По существу РЭБ присущи все элементы информационной войны. Отличия можно усмотреть, во-первых, в том, что проявление противоборства наблюдается между организационно-техническими системами и ведется радиоэлектронными средствами, во-вторых, в том, что ввиду ограниченности средств и объектов воздействия в ней до сих пор не использовались напрямую информационные операции типа ПСИОП, а лишь сопровождались ими. Во многом элементы стратегии и тактики РЭБ применяются в других информационных операциях, например, проводимых в компьютерных сетях.

В доктрине информационных операций РЭБ рассматривается и как средство нападения, и как средство защиты. **Средства РЭБ включают**:

- радиоэлектронную разведку, которая может производиться во всем спектре электромагнитного и оптического излучения, а также с применением радиотехнических средств для анализа механических и звуковых колебаний, магнитных полей;
- радиопротиводействие, направленное на подавление электромагнитного воздействия на собственные средства телекоммуникаций и управления;
- радиомаскировку, целью которой является активное и пассивное сокрытие электромагнитных излучений собственных радиоэлектронных средств и других систем;
- помехозащиту, предназначенную для активного влияния на системы управления оружием противника.

Оборонительные *информационные операции* проводятся с целью сохранения работоспособности собственных информационных телекоммуникационных систем, циркулирующей и хранящейся в них информации, а также предотвращения информационного воздействия на собственные системы управления и управляющие структуры. Они призваны гарантировать своевременный, точный и адекватный доступ к собственным информационным ресурсам и исключать возможности эксплуатировать противником собственную информацию и информационные системы для его целей.

Оборонительные ИО включают:

- защиту информационного обеспечения,
- операции по обеспечению секретности,
- физическую защиту информации и информационных систем,
- контробман,
- контрпропаганду,
- контрразведку,
- РЭБ и другие специальные информационные операции.

Защита информационного обеспечения направлена на достижение безопасности информации и информационных систем, гарантируя их доступность, целостность; на идентификацию и аутентификацию пользователей, конфиденциальность и надежность функционирования. Она обеспечивает восстановление информационных систем, включая защиту, обнаружение атак и возможные ответные реакции. Защита информационного обеспечения использует технологии и процессы типа многоуровневой защиты, управления доступом, безопасных сетевых технологий и программных средств обнаружения вторжения.

Оборонительные ИО содержат четыре взаимосвязанных процесса:

- защита информационной среды,
- обнаружение нападения,
- восстановление функционирования,
- ответные действия.

Для обеспечения эффективной обороны необходимо планирование и осуществление всех доступных информационных воздействий как наступательного, так и оборонительного характера в полной их интеграции. Стратегия и тактика применения наступательных информационных боевых средств и средств противодействия им постоянно совершенствуются. Об этом свидетельствуют многочисленные публикации в США, посвященные анализу проводимых информационных операций как в мирной фазе, так и в условиях конфликтов, а также разработке планов развития информационных боевых средств в период до 2025 г.

Наиболее опасным источником угроз информационной безопасности социальным, организационным и организационно-техническим системам являются угрозы, связанные с информационным воздействием. Наиболее подвержены скрытому информационному воздействию молодежь, малообразованные и пассивные слои социальных и организационных систем.

Вопросы:

1. Что является предметом учебной дисциплины «Методы и средства защиты компьютерной информации»?

Ответы:

a. являются принципы построения, организация применения эффективных средств и методов защиты информации на объектах ВТ войск ВКО; (Прав.)
b. является формирование у курсантов знаний и практических навыков по организации защиты информации и использованию различных методов и средств защиты компьютерной информации на объектах ВТ, в автоматизированных системах и сетях;
c. **:** является подготовка курсантов к эффективному использованию современных методов и средств защиты компьютерной информации на объектах вычислительной техники войск ВКО.

2. Какими составляющими характеризуются объекты защиты?

Ответы:

a. информацией; носителем защищаемой информации; информационным процессом. (Прав.)
b. информацией; средством защиты; источником защиты;
c. Информацией; данными; вредоносным ПО.

3. Что входит в возможные подразделы управления ЗИ:

Ответы:

a. управление техническими средствами и системами ЗИ; (Прав.)
b. организационно-техническая система ЗИ;
c. категории информации.

4. Какова главная цель учебной дисциплины «Методы и средства защиты компьютерной информации»?

Ответ:

a. являются принципы построения, организация применения эффективных средств и методов защиты информации на объектах ВТ войск ВКО;
b. является формирование у курсантов знаний и практических навыков по организации защиты информации и использованию различных методов и средств защиты компьютерной информации на объектах ВТ, в автоматизированных системах и сетях; (Прав.)
c. является подготовка курсантов к эффективному использованию современных методов и средств защиты компьютерной информации на объектах вычислительной техники войск ВКО.

5. Что понимают под процессом ЗИ?

Ответ:

a. совокупность действий по применению методов (способов) и средств ЗИ. (Прав.)
b. совокупность целенаправленных воздействий органов управления на объекты защиты, силы и средства ЗИ.

6. В чём заключается задача учебной дисциплины «Методы и средства защиты компьютерной информации»?

Ответ:

a. являются принципы построения, организация применения эффективных средств и методов защиты информации на объектах ВТ войск ВКО;
b. является формирование у курсантов знаний и практических навыков по организации защиты информации и использованию различных методов и средств защиты компьютерной информации на объектах ВТ, в автоматизированных системах и сетях;
c. является подготовка курсантов к эффективному использованию современных методов и средств защиты компьютерной информации на объектах вычислительной техники войск ВКО. (Прав.)

7. Что понимают под управлением ЗИ?

Ответ:

a. совокупность целенаправленных воздействий органов управления на объекты защиты, силы и средства ЗИ; (Прав.)
b. создание необходимых образовательных, научных, технических, информационных и других условий для реализации процесса ЗИ.

8. Что понимают под методом (способом) защиты информации?

Ответ:

a. понимают порядок и правила применения соответствующих принципов и средств ЗИ (Прав.)
b. совокупность действий для обеспечения информационной безопасности;
c. выбор средств защиты информации.

9. Что в себя включает обеспечение ЗИ (выберите правильный ответ)?

Ответ:

a. материально-техническое обеспечение деятельности органов и средств ЗИ, образовательную деятельность в области ЗИ, проведение НИОКР в области ЗИ, оказание услуг по ЗИ. (Прав.)
b. материально-техническое обеспечение деятельности органов и средств ЗИ, проведение НИОКР в области ЗИ, оказание услуг по ЗИ.
c. материально-техническое обеспечение деятельности органов и средств ЗИ, образовательную деятельность в области ЗИ, проведение НИОКР в области ЗИ, оказание услуг по ЗИ, проведение спец проверок защищаемых объектов .

10. Дайте определение защите ИПО:

Ответ:

a. использование средств и методов, принятие мер и осуществление мероприятий с целью обеспечения безопасности хранимой и обрабатываемой информации, а также используемых в ВС программных средств; (Прав.)
b. состояние информации, которое соответствует установленному статусу ее хранения и использования.

11. Дайте определение безопасности ИПО:

Ответ:

a. использование средств и методов, принятие мер и осуществление мероприятий с целью обеспечения безопасности хранимой и обрабатываемой информации;
b. это состояние информации, которое соответствует установленному статусу ее хранения и использования. (Прав.)

12. Что понимают под целостностью информации:

Ответ:

a. доступность их только для тех лиц, которые имеют на это соответствующие полномочия;
b. способность обеспечивать ее неизменность (физическая целостность) и непротиворечивость (логическая целостность) в процессе хранения и обработки данных (Прав.);
c. способность точно и своевременно выполнять все свои функции.

13. Что понимают под конфиденциальностью данных:

Ответ:

a. способность обеспечивать ее неизменность;
b. доступность их только для тех лиц, которые имеют на это соответствующие полномочия (Прав.)
c. способность точно и своевременно выполнять все свои функции.

14. Что понимают под надежностью программных средств:

Ответ:

a. способность обеспечивать ее неизменность;
b. доступность их только для тех лиц, которые имеют на это соответствующие полномочия;
c. способность точно и своевременно выполнять все свои функции. (Прав.)

Старший преподаватель 63 кафедры
к.т.н. м-р С.Краснов