Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий
Кафедра информационной безопасности и теории управления

А.М. Иванцов, В.Г Козловский

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. КУРС ЛЕКЦИЙ

Учебное пособие
Часть 1

Ульяновск
2019

Печатается по решению Ученого совета
факультета математики, информационных и авиационных
технологий Ульяновского государственного университета
(протокол № 4/19 от 21.05.2019г)

Рецензенты:

М.А. Волков – кандидат физико-математических наук,
ФГБОУ ВО «Ульяновский государственный университет»,
С.М. Бородин – кандидат технических наук,
ФГБОУ ВО «Ульяновский государственный технический университет».

Иванцов А.М., Козловский В.Г.

И 23 Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2019 – 4 с.

Рассматриваются лекции по курсу «Основы информационной безопасности» для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем».
Предназначено для студентов в качестве основного лекционного материала при изучении курса «Основы информационной безопасности».

УДК 004.056 (075.8)
ББК 32.972.53 я 73
И 23

Оглавление

Часть 1

В учебное пособие (Часть 2) будут включены следующие разделы и темы:

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ИБ – информационная безопасность;
НСД - несанкционированный доступ;
ЗИ - защита информации;
СМИ - средства массовой информации;
ПО - программное обеспечение;
АС - автоматизированная система;
ИС – информационная система;
СУБД – система управления базами данных;
ОС - операционная система;
ОТКС - открытые информационно-телекоммуникационные сети;
РЭП - радиоэлектронное подавление;
ИВ - информационное воздействие;
ИОБ системы - информационные обучающиеся системы;
НТВ – российский телевизионный канал;
СВТ - средства вычислительной техники;
ГТК - Гостехкомиссия при Президенте Российской Федерации;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ФСБ - Федеральная служба безопасности.

ВВЕДЕНИЕ

В учебное пособие включены лекционные материалы по курсу «Основы информационной безопасности для специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем».

Учебное пособие может быть полезно студентам, преподавателям и аспирантам, осваивающим вопросы защиты информации.

В учебное пособие включено 4 раздела (18 тем), направленных на освоение студентами специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем» основ информационной безопасности в соответствии с учебными планами.

Темы № 1-4,11,14-16 могут рекомендованы в ходе изучения дисциплины «Информационная безопасность и защита информации» для студентов по направлению 46.03.02 «Документоведение и архивоведение» (бакалавриат).

Темы № 3-4,16-18 могут рекомендованы в ходе изучения дисциплины «Обнаружение вторжений и защита информации» для студентов по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем» (бакалавриат).

Темы № 1-4, 9, 11, 14, 16-18 могут рекомендованы в ходе изучения дисциплины «Информационная безопасность» для студентов по направлению 09.03.03 «Прикладная информатика» (бакалавриат).

Темы № 1-10 могут рекомендованы в ходе изучения дисциплины для магистров по направлению 11.04.02 "Инфокоммуникационные технологии и системы связи".

Темы № 1-10 могут рекомендованы в ходе изучения дисциплины «Защита информации и информационная безопасность» для студентов направления 11.03.02 "Инфокоммуникационные технологии и системы связи" (бакалавриат), 09.03.02 Информационные системы и технологии (*бакалавр).*

РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕМА 1. ПОНЯТИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

1. Сущность и содержание национальной безопасности

2. Основные понятия и общеметодологические принципы информационной безопасности

Литература:

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. -392с.

2. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.

3. Стратегия национальной безопасности Российской Федерации **(**Указ Президента РФ от 31.01.2015 г. № 683).

4. Доктрина ИБ информационной безопасности РФ от 05.12.2016 (Указ Президента РФ от 05 декабря 2016 г.).

1. Сущность и содержание национальной безопасности

Национальная безопасность Российской Федерации - это то, что обеспечивает потенциал развития страны на длительный исторический период, а также стабильность и благополучие общества.

Национальная безопасность предполагает защищенность жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внутренних и внешних угроз.

Направления и задачи по обеспечению национальной безопасности определены в **Стратегии национальной безопасности РФ (**Указ Президента РФ от 31.01.2015 г. № 683). **Справка** (ранее было): - Концепция национальной безопасности РФ (Указ Президента РФ от 10 января 2000 г. № 24); - Стратегия национальной безопасности РФ до 2020 года (Указ Президента РФ от 12.05.2009 № 537).

Основными задачами в области обеспечения национальной безопасности РФ являются: - своевременное прогнозирование и выявление угроз национальной безопасности РФ; - реализация оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз; - обеспечение суверенитета и территориальной целостности РФ, безопасности ее пограничного пространства; подъем экономики страны, проведение независимого и социально ориентированного экономического курса; - преодоление научно-техничкой и технологической зависимостей РФ от внешних ис-

точников; - обеспечение на территории России личной безопасности человека и гражданина, его конституционных прав и свобод; - совершенствование системы государственной власти РФ, федеративных отношений, местного самоуправления и законодательства РФ, формирование гармоничных межнациональных отношений, укрепление правопорядка и сохранение социально-политической стабильности общества; - обеспечение неукоснительного соблюдения законодательства РФ всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями; - обеспечение равноправного и взаимовыгодного сотрудничества России, прежде всего с ведущими государствами мира; - подъем и поддержание на достаточно высоком уровне военного потенциала государства; - укрепление режима нераспространения оружия массового уничтожения и средств его доставки; - принятие эффективных мер по выявлению, предупреждению и пресечению разведывательной и подрывной деятельности иностранных государств, направленной против РФ; - коренное улучшение экологической ситуации в стране.

Для того, чтобы уяснить сущность и содержание национальной безопасности, дадим определение субъекта безопасности. **Субъектом безопасности** является тот, кто обладает правами и обязанностями по ее обеспечению; тот, кто защищает. Отсюда: О**бъект безопасности** - это то, что подлежит защите.

Действительно, любая социальная организация в результате как функционального (сословного), так и экономического (классового) неравенства объективно порождает систему, которую наделяет правами и обязанностями как по защите себя в целом от внешних опасностей, так по сдерживанию противоречий внутри себя самой.

Поскольку в нашем случае речь идет о национальной безопасности, то рассматриваемая социальная организация — это нация (общество. Это понятие ключевое для обозначения конкретной страны в рамках так называемой Вестфальской системы международных отношений.

Нация выступает и как субъект и как объект обеспечения безопасности. При этом для общества первостепенное значение имеет сохранение присущего ему и только ему образа жизни, для государства же определяющим является полнота его публичной власти и функции, выполняемых путем ее применения. Государство фактически управляет той и другой сторонами образа жизни общества, а при необходимости и защищает его. Об этом крас-

норечиво свидетельствуют внешние и внутренние функции государства — охранительные, регулятивные, оборонные.

Другими словами, **обеспечение безопасности четко проявляется в** функциях государства. В то же время общество располагает собственными (внегосударственными) механизмами обеспечения безопасности для поддержания нормальных общественных отношений, установленных нормативно-правовыми актами, обычаями и традициями, обеспечивающими достаточный уровень личной безопасности своих членов и самого общества в целом. С этих позиций объекты национальной безопасности — это функции государства и образ жизни общества. В этом контексте **национальная безопасность — это состояние взаимодействия общества и государства**, определяющее возможность воспроизводить присущие им функции и образ жизни в конкретных условиях обстановки. При этом **основными элементами национальной безопасности выступают**: - безопасность личности (ее права и свободы); общественная безопасность (материальные и духовные ценности общества); - государственная безопасность. Ее объекты — конституционный строй, суверенитет и территориальная целостность.

Основным же субъектом обеспечения национальной безопасности выступает государство, осуществляющее функции в этой области через органы власти. Так трактует объекты безопасности Закон РФ N 390-ФЗ 2010 года «О безопасности». В нашей стране термин «национальная безопасность» выступил развитием термина «безопасность», сформулированного в упомянутом законе. Этот термин впервые официально был использован в Федеральном законе «Об информации, информатизации и защите информации», который был принят в 1995 г. (С 2006 года название этого закона - «Об информации, информационных технологиях и о защите информации».

Действующий официальный термин «национальной безопасность» определен документом «Стратегия национальной безопасности РФ». В соответствии со Стратегией, национальная безопасность РФ (далее - **национальная безопасность**) - **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, эко-

логическую, экономическую, транспортную, энергетическую безопасность, безопасность личности;

Таким образом, сущность национальной безопасности определяется как состояние защищенности страны, которое возникает в процессе взаимодействия органов государственной власти, организаций и общественных объединений для защиты национальных интересов от угроз. Содержание же этого понятия образуют понятия «национальный интерес», «угроза национальной безопасности» и «система обеспечения национальной безопасности».

Национальные интересы РФ - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития.

Виды безопасности: в основу всякой классификации положены классификационные признаки. Среди них прежде всего следует выделить **объекты безопасности, характер угроз, сферы жизнедеятельности.**

В зависимости от объекта, жизненно важные интересы которого защищаются от внутренних и внешних угроз, выделяются такие виды безопасности, как **безопасность личности, общества, государства, русскоязычного населения, государственных служащих и т. д.**

При этом под безопасностью того или иного объекта имеется в виду защищенность жизненно важных интересов данного объекта от внутренних и внешних угроз.

Под безопасностью от того или иного вида угроз понимается защищенность жизненно важных интересов личности, общества и государства от угроз данного вида.

В человеческом обществе жизненно важные интересы всех объектов безопасности подвергаются воздействию самых различных угроз, поэтому особую практическую значимость имеет **подразделение видов безопасности по сферам или областям жизнедеятельности, в которых и проявляются эти угрозы.** Именно по этому принципу классифицированы жизненно важные интересы, угрозы и направления обеспечения национальной безопасности в Стратегии национальной безопасности РФ. В человеческом обществе жизненно важные интересы всех объектов безопасности подвергаются воздействию самых различных угроз, поэтому особую практическую значимость имеет **подразделение видов безопасности по сферам или областям жизнедеятельности, в которых и проявляются эти угрозы.** Именно по этому принципу классифицированы жизненно важные интересы, угрозы и направ-

ления обеспечения национальной безопасности в Концепции национальной безопасности Российской Федерации.

Наиболее обобщенно подобную классификацию можно ограничить выделением **пяти видов безопасности**, которые можно дробить на более мелкие виды безопасности по конкретным сферам жизнедеятельности (Рис. 1).

В этом случае под тем или иным видом безопасности понимается защищенность жизненно важных интересов личности, общества и государства в указанной сфере жизнедеятельности от внутренних и внешних угроз. Так, **военная безопасность** — это защищенность жизненно важных интересов личности, общества и государства в оборонной сфере от внутренних и внешних угроз. Соответственно, **экономическая безопасность** — это защищенность жизненно важных интересов личности, общества и государства в экономической сфере от внутренних и внешних угроз.

Аналогичным образом определяются и другие понятия. Подобный подход упорядочивает классификацию видов безопасности, дает возможность избегать существующего сейчас смешения принципов классификации и позволяет рассматривать национальную безопасность как единую систему видов безопасности, каждый из которых является самостоятельной подсистемой со своими характерными особенностями. Практика свидетельствует, что все эти подсистемы тесно связаны между собой и находятся в диалектическом взаимодействии. В практической деятельности по обеспечению национальной безопасности нельзя предавать забвению ни один из видов национальной безопасности, как это имело место, к сожалению, в недалеком прошлом, когда Советский Союз распался на пике своего военного могущества, достигнутого в ущерб экономической и социальной безопасности.

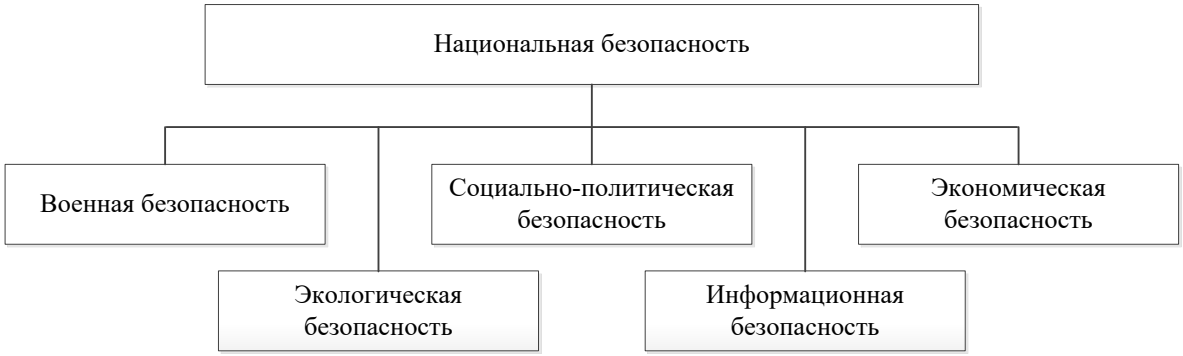

Рис. 1. Классификация видов национальной безопасности по сферам жизнедеятельности

Безусловно, на каждом этапе исторического развития приоритеты тех или иных видов безопасности объективно меняются, и потому важнейшей

задачей обеспечения национальной безопасности является достижение в каждый временной период определенного рационального паритета между различными видами безопасности.

2. Основные понятия и общеметодологические принципы ИБ

Под **информационной безопасностью (ИБ)** понимается - состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере, при котором обеспечиваются реализация конституционных прав и свобод граждан РФ, достойные качество и уровень их жизни, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства (Доктрина ИБ информационной безопасности РФ от 05.12.2016).

Укрепление информационной безопасности названо в Стратегии национальной безопасности РФ в числе важнейших долгосрочных задач.

Государственная политика обеспечения ИБ РФ основывается на следующих принципах:

1. Соблюдение Конституции и законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ.
2. Открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ.
3. Правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающемся на конституционном праве граждан, на свободный поиск, получение, передачу, производство и распространение информации любым законным способом.
4. Приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Основными составляющими ИБ являются защита информации (в смысле охраны персональных данных, государственной и служебной тайны и других видов информации ограниченного распространения, определенной законами РФ), предохранение информации от случайных или преднамеренных воздействий естественного или искусственного характера, реализация

гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, защищенность потребностей граждан, отдельных групп и населения в целом в качественной информации для их жизнедеятельности, образования и развития, г. е. информационно-психологическая удовлетворенность потребностей граждан и общества в целом и их защищенность от негативных (преднамеренных и случайных) информационно-психологических и информационно-технических воздействий.

В качестве иллюстрации места ИБ в обеспечении национальной безопасности можно представить рисунок (кольцо, на котором по кругу изображены, например, **геополитическая, оборонная, политическая, социальная, экономическая, продовольственная, демографическая, экологическая, культурная и психологическая безопасности**). Где ИБ? Внутри круга.

Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Для достижения этого осуществляется: - обеспечение конституционных прав и свобод человека на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, защиты своей чести и своего доброго имени; - развитие современных информационных технологий, отечественной индустрии информации; - повышение безопасности информационных систем федеральных органов государственной власти, органов государственной власти субъектов РФ, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами; - защита информационных ресурсов от несанкционированного доступа (НСД); - развитие отечественного производства технических средств защиты информации (ЗИ); - защита сведений, составляющих государственную тайну. Важной сферой безопасности информации является защита прав собственности на нее. Федеральным законом «Об информации, информационных технология и о защите информации» определено, что информационные ресурсы, т. е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государства, подлежат обязательному учету и защите как материальное имущество собственника.

Вся информация с точки зрения права делится на:

общедоступную (информацию без ограничения права доступа). К такого рода информации, например, относится информация общего пользования, информация о состоянии окружающей среды, ее загрязнении, информация в области работ по хранению, перевозке, уничтожению химического оружия и др. Информация, содержащая сведения об обстоятельствах и фактах, представляющих угрозу жизни, здоровью граждан, не подлежит засекречиванию, не может быть отнесена к тайне;

- **информацию с ограниченным доступом -** государственная тайна, служебная информация, коммерческая, банковская и профессиональная тайны и персональные данные;
- **информацию, распространение которой наносит вред интересам общества, законным интересам и правам граждан.** К ней относится порнография; информация, разжигающая национальную, расовую и другую рознь; пропаганда и призывы к войне; ложная реклама и т. п.;
- **объекты интеллектуальной собственности** — то, что не может быть отнесено к информации с ограниченным доступом, но охраняется особым порядком через институты интеллектуальной собственности — авторское право, патентное право и т. п. Исключение составляют профессиональные секреты, которые охраняются в режиме коммерческой тайны.

К ограничениям и запретам следует отнести следующие перечни.

1. Перечень оснований для ограничения информационных прав: - защита основ конституционного строя; - защита нравственности, здоровья, прав, законных интересов других лиц; - обеспечение обороны страны и безопасности государства; - обеспечение общественного спокойствия в целях предотвращения беспорядков и борьбы с преступностью; - предотвращение разглашения конфиденциальной информации; - обеспечение авторитета и беспристрастности правосудия; - условия чрезвычайного положения, установленные по закону (на определенный период).

2. Перечень случаев прямого ограничения информационных прав: - использование прав в целях насильственного изменения конституционного строя; - пропаганда социальной ненависти, социального, расового, национального, религиозного, языкового превосходства, насилия и войны; - нарушение на неприкосновенность частной жизни (на личную, семейную тайну), неприкосновенность жилища, права на уважение чести, достоинства и репутации, тайны переписки, телефонных переговоров, телеграфных и иных сообщений; - нарушение права на государственную, служебную, профессиональную, ком-

мерческую и банковскую тайны; - право на отказ от свидетельствования против себя самого, своего супруга и близких родственников.

3. Перечень видов информации с ограниченным доступом: государственная тайна; служебная тайна; коммерческая тайна; банковская тайна; профессиональная тайна; персональные данные.

Контрольные вопросы

1. В чём заключается сущность национальной безопасности РФ?
2. Какие документы определяют национальную безопасность РФ?
3. Кратко охарактеризовать основные виды национальной безопасности по сферам жизнедеятельности.
4. Пояснить основные общеметодологические принципы ИБ.
5. Перечислить основания для ограничения информационных прав.
6. Назвать примеры информации с ограниченным доступом.

ТЕМА 2. НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ

1. Место и роль России в глобальном информационном пространстве

2. Национальные интересы РФ в информационной сфере и их обеспечение

Литература:

1. Стратегия национальной безопасности Российской Федерации: Утв. Указом Президента РФ от 31 декабря 2015г. № 683.
2. Доктрина информационной безопасности Российской Федерации: Утв. Указом Президента РФ от 05 декабря 2016 г.
3. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.
4. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.:РИОР: ИНФРА-М, 2015. -392с.

1. Место и роль России в глобальном информационном пространстве

Эффективность осуществления власти в любом государстве, в том числе в РФ, в немалой степени зависит от его информационного обеспечения. Без информации невозможно представить позитивно функционирующую политическую структуру, развитие массового политического сознания, взаимодействие субъекта и объекта политики. Вполне очевиден тот факт, что отставание страны в области технологий информационной политики не может содействовать успеху в решении поставленных задач.

В качестве правовых норм закреплены положения Стратегии национальной безопасности РФ, в которой существенное внимание отдается информационных угрозам, а также Доктрина информационной безопасности РФ, которая содержит в себе перечень информационных угроз и направления деятельности федеральных органов власти по их предотвращению.

Сам факт существования этих нормативно-правовых актов говорит о важности и актуальности разработок, в том числе научно-теоретических, касающихся межгосударственных конфликтов в информационной сфере. Конечно, следует учесть, что конфликты в информационной сфере напрямую связаны с политическими конфликтами и экономическим соперничеством. И, как правило, каждое из противоречий нужно рассматривать комплексно.

2. Национальные интересы РФ в информационной сфере и их обеспечение

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, 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, упрочении демократии, 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 информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

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

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая включает в себя **соблюдение конституционных прав и свобод человека и гражданина в области получения инфор-**

мации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая включает **информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ**, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая включает **развитие современных информационных технологий, отечественной индустрии информации**, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая составляющая включает **защиту информационных ресурсов от НСД, обеспечение безопасности информационных и телекоммуникационных систем** (развернутых и создаваемых на территории России).

По мнению ряда авторитетных экспертов, на сегодняшний день **в сфере информационных процессов проявляются следующие тенденции**: - возрастает объем процессов, которые вытесняют традиционные информационно-пропагандистские способы влияния на массы; - налицо переплетение различных носителей информации (печатных, аудиальных, визуальных), т.е. возникновение интегрированных коммуникативных систем; - аналогичные процессы происходят и на уровне массовых информационных процессов, где возникают и развиваются уже не отдельные средства массовой информации (СМИ), а информационные комплексы, называемые медиа-системами.

Результатом глобальной информатизации общества становится образование единого информационного пространства. Информационное пространство представляет собой совокупность баз данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей.

Говоря о развитии информационного пространства, в качестве основных тенденций следует выделить Интернетизацию и глобализацию.

Что касается Интернета, то всемирная информационная паутина еще не стала всеобъемлющей, но она уже сегодня оказывает большое влияние на нашу жизнь. Этот процесс идет быстрее, чем можно себе представить. Из технического изобретения он превратился в абсолютный феномен, влияющий на все стороны жизни человечества. Не вызывает никаких сомнений тот факт, что развитие Интернет-технологий открывает перед обществом множество перспектив и дает надежду на качественный прорыв в самых разных сферах. Феномен интернета сегодня невозможно не учитывать и в политике.

Удельный вес виртуальной информационной составляющей в политике имеет устойчивую тенденцию к возрастанию. Этот процесс будет продолжаться и в будущем: количество сайтов политических партий и движений будет увеличиваться, информационная роль интернета вследствие этого будет возрастать. Что касается глобализации, то развитие этого процесса уже позволяет говорить о глобальном информационном обществе и едином информационном пространстве. Группа стран, таких, как США, Канада, Япония, Германия, Франция, Англия, Италия, рассматривая создание единого информационного пространства как одной из приоритетных задач XXI в., договорилась о сотрудничестве в создании глобальной информационной инфраструктуры.

Это сотрудничество опирается на несколько **основополагающих принципов**, в числе которых: поддержка динамичной конкуренции, обеспечение открытого доступа к сетям (услугам), признание необходимости международного сотрудничества, особенно с менее развитыми странами.

В настоящее время в мире сложилось **несколько основных региональных центров специализации по производству информационных продуктов и высокотехнологичных компонентов:** - это Североамериканское сообщество, включающее в себя США и Канаду, которые лидируют в производстве новых программных продуктов для широкого использования и разработках новых образцов компьютерной техники; - страны Европейского союза, специализирующиеся на рынке коммуникаций; - это традиционно Япония со странами Юго-Восточной Азии, Китай и Индия. Все они обладают производственными мощностями и сравнительно дешевой рабочей силой и являются массовыми поставщиками элементов компьютерной продукции.

Страны Содружества Независимых Государств (СНГ), в этом международном разделении труда, к сожалению, играют пока, в основном, роль потребителя. Это дает основание некоторым экспертам и политикам скептично

относится к идее вхождения этих стран в мировое информационное сообщество.

Сторонники информационной глобализации указывают на то, что появление глобального информационного пространства означает приближение эпохи глобальной экономики, которая будет характеризоваться "стиранием" географических границ рынков сбыта, появлением распределенных сетевых трудовых ресурсов, кардинальным сближением производства и потребления, открытием новых рынков в новой сфере интеллектуального потребления, что, естественно, повлечет за собой совершенно новые возможности.

Без единого информационного пространства, создающего взаимовыгодную интеграционную основу для развития делового сотрудничества во всех областях политической, экономической и культурной жизни, интеграция государств становится весьма проблематичной. Не вызывает сомнений, что рыночная экономика – прежде всего, информационная экономика. Свидетельством тому является весь послевоенный опыт развития мировой экономики.

Всё это поднимает вопрос ИБ, от обеспечения которой во многом будет зависеть перспектива развития СНГ. В настоящий момент на карту поставлено будущее стран СНГ: будем ли мы находиться "на задворках" мирового информационного сообщества или же сумеем занять свою нишу в веке информации?

Обеспечение ИБ является одним из важных вопросов как отдельных государств, так и всего СНГ. Для обеспечения безопасности в информационной сфере необходимо определить, какая именно, откуда и по каким причинам может исходить эта угроза. Возникновению угрозы ИБ могут способствовать как внешние, так и внутренние факторы. К внешним факторам можно отнести глобальный процесс информатизации, и вытекающие из него последствия, к примеру, в виде информационных потоков, которые могут неблагоприятно отразиться на общественном сознании и на имидже государства.

К внутренним факторам можно отнести состояние информационного пространства, уровень развития информационной инфраструктуры, а также нормативно-правовое регулирование информационной сферы.

В целом для обеспечения ИБ и формирования устойчивого к вызовам информационного пространства необходимы следующие шаги:

Первый - формирование единого информационно-коммуникационного пространства СНГ как части мирового информационного пространства, пол-

ноправное участие в процессах информационной и экономической интеграции регионов, стран и народов. **Второй** - становление и в последующем доминирование в экономике новых технологических укладов, базирующихся на массовом использовании перспективных информационных технологий, средств вычислительной техники и телекоммуникаций. **Третий** - создание и развитие рынка информации и знаний как факторов производства в дополнение к рынкам природных ресурсов, труда и капитала, переход информационных ресурсов общества в реальные ресурсы социально-экономического развития, фактическое удовлетворение потребностей общества в информационных продуктах и услугах. **Четвертый** - возрастание роли информационно-коммуникационной инфраструктуры в системе общественного производства. **Пятый** - повышение уровня образования, научно-технического и культурного развития за счет расширения возможностей систем информационного обмена на международном, национальном и региональном уровнях и соответственно повышение роли квалификации, профессионализма и способностей к творчеству как важнейших характеристик услуг труда. **Шестой** - создание эффективной системы обеспечения прав граждан и социальных институтов на свободное получение, распространение и использование информации как важнейшего условия демократического развития.

Однако все эти понятные и необходимые шаги вступают в противоречие с существующими реалиями. К сожалению, во многих странах СНГ система СМИ выступает в качестве механизма обслуживания конъюнктурных интересов власти и бизнеса, существуют значительные возможности их влияния на СМИ, отсутствуют методы регулирования уровня концентрации и монополизации СМИ, не разработана система защиты интересов региональных рынков массовой информации. Актуальными остаются вопросы совершенствования национальных законодательств в части гарантий свободы слова и информации, свободного распространения массовой информации, в том числе на трансграничном уровне, недопущения распространения насилия и нетерпимости через СМИ, обеспечения плюрализма СМИ, доступа к официальной информации.

Таким образом, наличие благоприятной атмосферы на информационном пространстве СНГ зависит от четкого обеспечения ИБ. В данном процессе активное участие должны принимать все страны содружества и региона, всесторонне рассматривая вопросы, касающиеся обеспечения ИБ, и создавая с учетом прошлого опыта усовершенствованную нормативно-правовую базу.

Наиболее важным ресурсом, оказывающим все большее влияние на национальную безопасность, становится информация, циркулирующая в автоматизированных системах управления и связи.

Данные системы являются неотъемлемым компонентом структуры управления государством, экономикой. Финансами и обществом. Они становятся основой управления жизнедеятельностью и жизнеобеспечением стран и континентов. В тоже время во все большей степени развертывается межгосударственная борьба за лидерство в информационной сфере.

В международных отношениях давно в ходу такие понятия. Как " информационная война", " информационные войска", " информационное противоборство", " информационная операция". Возрастание роли и значения информационной составляющей в структуре военной безопасности и безопасности войск обусловлено общемировой тенденцией продвижения передовых стран к так называемому информационному обществу, где информация и информационные услуги будут основным фактором политического, экономического и социального развития.

Контрольные вопросы

1. Какова значимость информационного обеспечения для государства?
2. Роль России в глобальном информационном пространстве.
3. Интересы личности, общества и государства в информационной сфере.
4. Составляющие национальных интересов РФ в информационной сфере.
5. Пояснить что такое единое информационное пространство как результат глобальной информатизации общества.
6. Перечислить первоочередные шаги РФ в области ИБ для формирования устойчивости к вызовам информационного пространства.

ТЕМА 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Проблемы обеспечения информационной безопасности

2. Потенциальные угрозы информации

3. Классификация угроз и каналов утечки информации

4. Неформальная модель нарушителя

Литература:

1. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.

2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.:РИОР: ИНФРА-М, 2015. -392с.

1. Проблемы обеспечения информационной безопасности

В современном мире бурно развиваются технологии обработки, хранения и передачи информации. Применение информационных технологий требует повышенного внимания к вопросам ИБ. Уничтожение информационных ресурсов, их недоступность или несанкционированное использование вследствие нарушений ИБ, вызывают серьезные проблемы у граждан, социальных групп, компаний и государств.

Проблемы ИБ можно разделить на три больших группы:

1. Проблемы гуманитарного характера, возникающие в связи с бесконтрольным использованием и распространением персональных данных, вторжениями в частную жизнь, клеветой и др. относительно конкретной личности.
2. Проблемы экономического и юридического характера, возникающие в результате утечки, искажения и потери коммерческой и финансовой информации, кражи брендов и интеллектуальной собственности, раскрытия информации о материальном положении граждан, промышленного шпионажа и распространения материалов, наносящих ущерб репутации компаний.
3. Проблемы политического характера, возникающие из-за информационных войн, кибервойн, электронной разведки в интересах политических групп, компрометации информации ограниченного доступа, атак на информационные системы важных оборонных и промышленных объектов, неполного информирования и дезинформации руководителей крупных учреждений.

В последние годы проблематика ИБ пополнилась такими сложными задачами, как: – разработка и реализация надёжных систем электронной подписи, электронных выборов, закупок и платежей; – создание и внедрение передовых средств аутентификации; – разработка и внедрение новых методов обеспечения надежности и отказоустойчивости (инновационные технологии кластеризации, виртуализации и др.); – защита беспроводных соединений, мобильных устройств и «умной» электроники; – обеспечение безопасности веб-сервисов и «облачных» технологий; – защита от вирусных и хакерских атак, направленных на конкретные предприятия; – разработка новых стойких систем шифрования; – борьба с современными изощренными методами «черного» пиара, мошенничества и дезинформации в цифровом пространстве.

Решение указанных острых проблем в области ИБ возможно только при условии: – внимания к данным вопросам и надлежащих, целенаправленных действий руководителей компаний, представителей общественности и государственной власти; – согласованной деятельности национальных и ме-

ждународных органов, занимающихся стандартизацией ИБ и борьбой с киберпреступностью.

2. Потенциальные угрозы информации

Угроза безопасности информации – это потенциальная возможность нарушения основных качественных характеристик (свойств) информации при ее обработке техническими средствами: конфиденциальности, целостности, доступности.

Таким образом, понятие «угроза» заключается в образовании каких-либо обстоятельств, условий, процессов, влияющих на информацию, имеющую определенную сущность.

Если информация представляет ценность, то необходимо понять, в каком смысле эту ценность необходимо оберегать. Если ценность информации теряется при ее раскрытии, то говорят, что имеется опасность нарушения конфиденциальности информации.

Если ценность информации теряется при изменении или уничтожении информации, то говорят, что имеется опасность для целостности информации.

Если ценность информации в ее оперативном использовании, то говорят, что имеется опасность нарушения доступности информации.

Если ценность информации теряется при сбоях в системе, то говорят, что есть опасность потери устойчивости к ошибкам.

Обычно рассматривают первые три опасности, которые надо предотвратить путем защиты: конфиденциальность, целостность и доступность.

Естественно, что угроза информации может возникнуть по вполне определенным причинам (факторам). Как известно, слово «фактор» происходит от латинского «factor – делающий, производящий» и обозначает движущую силу, причину какого-либо процесса, явления.

Множество факторов опасности (причин возникновения угроз) можно свести в три основных группы:

1. Природные факторы, вызываемые физическими воздействиями стихийных природных явлений (наводнения, землетрясения, магнитные бури, радиоактивные излучения и т.д.). Названные факторы в большинстве случаев неявно зависят или вообще не зависят от деятельности человека.

2. Технические факторы, вызываемые сопутствующими работе радиоэлектронной аппаратуры побочными электромагнитными излучениями и их наводками на окружающие металлические предметы, ошибками в проектировании, в программном обеспечении, случайными сбоями в работе ПЭВМ и

линий связи, энергопитания, воздействием на аппаратуру физических полей при несоблюдении условий электромагнитной совместимости и т.д.. Эти факторы опосредованно зависят от деятельности человека, хотя, сбои в работе оборудования и пропадания энергопитания могут быть вызваны целенаправленно.

3. Социальные факторы, обусловленные происходящими в обществе экономическими, политическими, нравственными изменениями и проявляющиеся в виде ошибок пользователей, несанкционированных действий обслуживающего персонала и несанкционированного воздействия на ресурсы информационных систем как со стороны своих сотрудников (внутренний нарушитель), так и посторонними лицами (внешний нарушитель), либо теми и другими, действующими в сговоре. Данные факторы непосредственно зависят от деятельности человека.

Угрозы конфиденциальности. Существует только два пути нарушения конфиденциальности (секретности): утрата контроля над системой защиты; каналы утечки информации. Каналы утечки характеризуют ту ситуацию, когда, либо проектировщики не смогли предупредить, либо система не в состоянии рассматривать такой доступ как запрещенный. Утрата управления системой защиты может быть реализована оперативными мерами, и здесь играют существенную роль административные и кадровые методы защиты. Утрата контроля за защитой может быть создана стихийно или искусственно. Поэтому одной из главных опасностей для систем защиты является отсутствие устойчивости к ошибкам. Утрата контроля может возникнуть за счет «взламывания» самой системы защиты. Противопоставить этому можно только создание защищенного домена для системы защиты.

Угрозы целостности. Нарушения целостности информации – это незаконные уничтожения или модификация информации. Традиционно защита целостности относится к категории организационных мер. Основным источником угроз целостности являются пожары и стихийные бедствия. К уничтожению и модификации могут привести также случайные и преднамеренные критические ситуации в системе, вирусы, атаки хакеров, неисправности и т.д. Язык описания угроз целостности обычно аналогичен языку угроз конфиденциальности. Однако, в данном случае вместо каналов утечки удобнее говорить о каналах воздействия на целостность (или о каналах разрушающего воздействия). Наконец, к механизмам контроля и защиты целостности информации следует отнести создание системной избыточности. В военной практике такие меры называются: повышение «живучести» системы. Ис-

пользование таких механизмов позволяет также решать задачи устойчивости к ошибкам и задачи защиты от нарушений доступности. Угроза целостности информации подразумевает защиту как самой информации, так и различных носителей, средств обработки и передачи информации.

3. Классификация угроз и каналов утечки информации

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные). Естественные угрозы - угрозы, вызванные воздействиями на автоматизированную систему (АС) и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

• непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АС и ее элементов, ошибками в ПО, ошибками в действиях персонала и т.п.;

• преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к АС могут быть внешними или внутренними (компоненты самой АС - ее аппаратура, программы, персонал, конечные пользователи).

Основные непреднамеренные искусственные угрозы (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим не-

обоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
6) заражение компьютера вирусами;
7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, идентификационных карточек, пропусков и т.п.);
9) игнорирование организационных ограничений (установленных правил) при работе в системе;
10) вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
11) неумышленное повреждение каналов связи и др.

Основные преднамеренные искусственные угрозы:

1) физическое разрушение системы (путем взрыва, поджога и др.) или вывод из строя наиболее важных компонентов компьютерной системы (устройств, носителей важной информации, лиц из числа персонала и т.п.);
2) отключение или вывод из строя подсистем обеспечения функционирования АС (электропитания, охлаждения и вентиляции, линий связи и т.п.);
3) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка активных радиопомех на частотах работы устройств системы и т.п.);
4) внедрение агентов в число персонала (в том числе, возможно, и в административную группу, отвечающую за безопасность);
5) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
6) применение подслушивающих устройств, дистанционная съемка и т.п.;
7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сели питания, отопления и т.п.);
8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
9) хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

10) несанкционированное копирование носителей информации;
11) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
12) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");
13) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи и т.п.;
14) вскрытие шифров криптозащиты информации;
15) внедрение аппаратных "спецвложений", программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему зашиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
16) незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо. Прямые каналы могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов.

По типу основного средства, используемого для реализации угрозы, все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

По способу получения информации потенциальные каналы доступа можно разделить на: - физический; - электромагнитный (перехват излучений); информационный (программно-математический).

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам АС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к ПО (в том числе к операционным системам), а также путем подключения к линиям связи.

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением устройств отображения информации, прослушиванием переговоров персонала АС и пользователей.

4. Неформальная модель нарушителя

Преступления, в том числе и компьютерные, совершаются людьми. В этом смысле вопросы безопасности АС есть суть вопросы человеческих отношений и человеческого поведения. Пользователи системы и ее персонал, с одной стороны, являются составной частью (необходимым элементом АС). С другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений.

Исследования проблемы обеспечения безопасности АС ведутся в направлении раскрытия природы явлений, заключающихся в нарушении целостности и конфиденциальности информации, дезорганизации работы компьютерных систем. Серьезно изучается статистика нарушений, вызывающие их причины, личности нарушителей, суть применяемых ими приемов и средств, недостатки систем и средств их защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы, которые могут быть использованы при построении моделей потенциальных нарушителей.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлении.

Нарушитель - лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольст-

вия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

При разработке модели нарушителя определяются: • предположения о категориях лиц, к которым может принадлежать нарушитель; • предположения о мотивах действий нарушителя (преследуемых нарушителем целях); • предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах); • ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа персонала и пользователей системы) или внешними (посторонними лицами).

Внутренним нарушителем может быть лицо из следующих категорий сотрудников: • конечные пользователи (операторы) системы; • персонал, обслуживающий технические средства (инженеры, техники); • сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты); • сотрудники службы безопасности АС; • руководители различных уровней.

Посторонние лица, которые могут быть нарушителями: • технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС); • клиенты и посетители (представители организаций, граждане); • представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию; • лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);

• любые лица за пределами контролируемой территории.

Можно выделить несколько основных мотивов нарушений: • безответственность; • самоутверждение; • вандализм; • принуждение; • месть; • корыстный интерес; • идейные соображения.

По уровню знаний об АС нарушителей можно классифицировать следующим образом: • знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами; • обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

• обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем; • знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам): • применяющий только агентурные методы получения сведений; • применяющий пассивные средства (технические средства перехвата без модификации компонентов системы); • использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны; • применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия: • в процессе функционирования АС (во время работы компонентов системы); • в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.); • как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия: • без доступа на контролируемую территорию организации; • с контролируемой территории без доступа в здания и сооружения;

• внутри помещений, но без доступа к техническим средствам АС; • с рабочих мест конечных пользователей (операторов) АС; • с доступом в зону данных (серверов баз данных, архивов и т.п.); • с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие **ограничения и предположения** о характере действий возможных нарушителей: • работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей; • нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников.

Контрольные вопросы

1. Характеристика проблем обеспечения информационной безопасности.
2. Основные условия решения острых проблем в области ИБ.

3. Угрозы безопасности информации. Привести примеры характерных угроз.
4. Пояснить на примерах основные свойства информации при ее обработке техническими средствами: конфиденциальность, целостность и доступность.
5. Какие факторы опасности (причины возникновения угроз) Вы знаете?
6. Пояснить классификацию естественных и искусственных угроз.
7. Привести 5 примеров основных непреднамеренных искусственных угроз.
8. Привести 5 примеров основных преднамеренных искусственных угроз.
9. Назвать основные потенциальные каналы доступа к информации.
10. Назвать основные потенциальные каналы утечки информации.
11. Дать характеристику неформальной модели нарушителя.
12. Раскрыть основное предназначение неформальной модели нарушителя. Дать примеры внешних и внутренних нарушителей.

ТЕМА 4. ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Источники угроз информационной безопасности РФ

2. Классификация источников угроз информационной безопасности

3. Классификация уязвимостей информационных систем

Литература:

1. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.
2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.:РИОР: ИНФРА-М, 2015. -392с.

Организация обеспечения ИБ должна носить комплексный характер. Она основывается на глубоком анализе негативных последствий. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, уязвимостей (факторов, способствующих их проявлению) и, как следствие, определение актуальных угроз ИБ.

Исходя из этого, моделирование и классификация источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия следующей логической цепочки (Рис. 1.1):

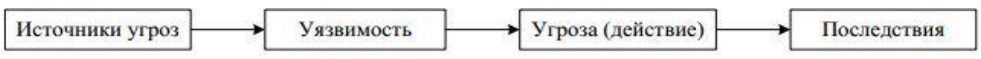

Рис. 1.1. Логическая цепочка угроз и их проявлений

Источники угроз - потенциальные антропогенные, техногенные и стихийные угрозы безопасности.

Под угрозой (в целом) понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим–либо интересам.

Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты ИС может прямо или косвенно привести к нанесению ущерба интересам субъектов.

Уязвимости – это присущие объекту информационной системы причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информационной системы, свойствами архитектуры информационной системы, протоколами обмена и интерфейсами, применяемым ПО и аппаратной платформы, условиями эксплуатации, невнимательностью сотрудников.

Последствия - результат реализации угрозы через уязвимости.

1. Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние.

К внешним источникам относятся:

- иностранные политические, экономические, военные, разведывательные и информационные структуры, действия которых направлены против интересов РФ в информационной сфере;
- международные террористические организации;

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности органов государственной власти по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность органов государственной власти в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации органов государственной власти в кредитно-финансовой сфере, промышленности, сельском хозяйстве, образовании, здравоохранении, сфере услуг и быта граждан.

Рассмотрим вариант классификации источников угроз, который будем использовать в процессе изучения дисциплины.

2. Классификация источников угроз информационной безопасности

Носителями угроз ИБ являются источники угроз. В качестве источников угроз могут выступать как субъекты, так и объективные проявления.

Все источники угроз ИБ целесообразно разделить на три основные группы.

I. Обусловленные действиями субъекта (**антропогенные источники**) – субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления.

Источники, действия которых могут привести к нарушению безопасности информации, могут быть как внешними, так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры.

2. Обусловленные техническими средствами (**техногенные источники**). Эти источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз ИБ также могут быть как внутренними, так и внешними.

3. **Стихийные источники.** Данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия, или др. обстоятельства, которые невозможно предусмотреть или предотвратить или можно

предусмотреть, но невозможно предотвратить). Эти обстоятельства носят объективный и абсолютный характер. Такие источники угроз совершенно не поддаются прогнозированию и меры против них должны применяться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

3. Классификация уязвимостей информационных систем

Угрозы, как правило, появляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности в ИС.

Уязвимости, присущие ИС, неотделимы от неё, и обуславливаются недостатками процесса функционирования, свойствами архитектуры ИС, протоколами обмена и интерфейсами, применяемым ПО и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации).

Устранение или существенно ослабление уязвимостей, влияет на возможности реализации угроз безопасности информации.

Существует следующая классификация уязвимостей:

1. **Объективные**, которые зависят от особенностей построения и технических характеристик оборудования, применяемого в ИС.
2. **Субъективные**, зависящие от действий сотрудников, которые, в основном, устраняются организационными мероприятиями и программно-аппаратными методами.
3. **Случайные -** зависят от особенностей окружающей ИС среды и непредвиденных обстоятельств.

Полное устранение объективных уязвимостей невозможно, они могут существенно ослабляться **техническими и инженерно-техническими методами.** К ним можно отнести:

1.1. Сопутствующие техническим средствам излучения:

- **электромагнитные** (побочные излучения элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей);
- **электрические** (наводки электромагнитных излучений на линиях и проводке, просачивание сигналов в сети электропитания, в цепи заземления, неравномерность потребления тока электропитания и др.);
- **звуковые** (акустические и виброакустические).

1.2. Активизируемые:

- **аппаратные закладки,** устанавливаемые в телефонные линии, в сети электропитания, в защищаемые помещения, в технические средства;
- **программные закладки** (вредоносные программы, технологические выходы из программ, нелегальные копии ПО).

1**.3. Определяемые особенностями элементов:**

- **элементы, обладающие электроакустическими преобразованиями** (телефонные аппараты, громкоговорители, микрофоны и др.);
- **элементы подверженные воздействию электромагнитного поля** (магнитные носители, микросхемы и др.).

1.4. Определяемые особенностями защищаемого объекта:

- **местоположением объекта** (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта);
- **организацией каналов обмена информацией** (использование радиоканалов, глобальных информационных сетей, арендуемых каналов).

2. Субъективные уязвимости, зависящие от действий сотрудников, в основном устраняются организационными и программно-аппаратными методами в процессе следующих действий:

2.1. Ошибки:

- **при подготовке и использовании ПО** (при разработке алгоритмов и ПО, инсталляции и загрузке ПО, эксплуатации ПО и вводе данных);
- при управлении сложными системами (при использовании возможностей самообучения систем, организация управления потоками обмена информации);
- при эксплуатации технических средств (при включении/выключении технических средств, использовании технических средств охраны, использование средств обмена информацией и др.).

2.2. Нарушения:

- режима охраны и защиты (доступа на объект, доступа к техническим средствам);
- режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения и др.);
- режима использования информации (обработка и обмен информацией, хранение и уничтожение носителей информации, уничтожения роизводственных отходов и брака);
- режима конфиденциальности (сотрудники работают в нерабочее время; уволенные сотрудники; обиженные сотрудники и др.).

3. Случайные уязвимости (зависят от особенностей окружающей ИС среды и непредвиденных обстоятельств):

3.1. Сбои и отказы:

- отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа);
- старение и размагничивание носителей информации (дискет, съемных носителей, жестких дисков, микросхем, кабелей и соединительных линий);
- сбои ПО (операционных систем (ОС), систем управления базами данных (СУБД), прикладных программ, сервисных и антивирусных программ);
- сбои электроснабжения (оборудования, обрабатывающего информацию, обеспечивающего и вспомогательного оборудования).

3.2. Повреждения:

- **жизнеобеспечивающих коммуникаций** (электро-, водо-, газо-, теплоснабжения, канализации; кондиционирования и вентиляции);
- ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий; корпусов технологического оборудования).

Контрольные вопросы

1. Пояснить на 2-3 примерах логическую цепочку угроз и их проявлений.
2. Дать определения угрозы, источника угроз, уязвимости и последствий реализации угроз.
3. Дать характеристику источникам внутренних и внешних угроз информационной безопасности РФ.
4. Пояснить выбранный вариант классификации источников угроз информационной безопасности.
5. Охарактеризовать антропогенные источники угроз и основные меры по их нейтрализации.
6. Охарактеризовать техногенные источники угроз и основные меры по их нейтрализации.
7. Охарактеризовать стихийные источники угроз и основные меры по их нейтрализации.
8. Привести примеры уязвимостей, присущих информационным системам.
9. Пояснить выбранный вариант классификации уязвимостей информационной системы.

РАЗДЕЛ 2. ИНФОРМАЦИОННАЯ ВОЙНА, МЕТОДЫ И СРЕДСТВА ЕЁ ВЕДЕНИЯ

ТЕМА 5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО

1. Проблемы информационной войны

2. Субъекты информационного противоборства

3. Составные части и методы информационного противоборства

Литература:

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. - 392с.

2. Малюк А.А. Защита информации в информационном обществе. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2015. – 230 с.

3. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 с.

1. Проблемы информационной войны

Информационно-психологическое воздействие существует столько времени, сколько существует сам человек. Воюющие стороны издавна знали, что бороться с неприятелем можно не только вооруженными средствами, но и путем целенаправленного воздействия на психику воинов. Основы ведения психологической войны были сформулированы еще в Трое. Всем известна знаменитая легенда о троянском коне. После десяти лет изнурительной войны и осады в одно прекрасное утро троянцы, не веря своим глазам, увидели, что лагерь греков пуст, а на берегу стоит огромный деревянный конь с надписью: «В благодарность за будущее благополучное возвращение домой ахейцы посвящают этот дар Афине». Жрец Лаокоон, увидев этого коня и, зная хитрости данайцев, воскликнул: «Что бы это ни было, я боюсь данайцев, даже дары приносящих!» Но троянцы, не слушая предостережений Лаокоона и пророчицы Кассандры, втащили коня в город. Древние люди относились к священным дарам с большим уважением и почтением, и, по решению царя Приама, конь был внесен в город и водворен в посвященной Афине цитадели. С приходом ночи сидевшие в коне вооруженные ахейцы выбрались наружу и напали на спящих жителей города. Так, благодаря коню, была захвачена Троя, так закончилась Троянская война. За ночь была достигнута та цель, которую тщетно добивались осаждавшие в течение 10 лет. Сейчас наиболее коварный компьютерный вирус-разрушитель так и называют – троянский конь.

Первая мировая война стала поворотным событием в развитии теории и практики информационного противоборства. В 1914 году в Великобритании было создано бюро военной пропаганды, а во Франции в 1915 году – отдел службы военной пропаганды. Обе организации в основном отвечали за

воздействие на противника с помощью листовок.

Типичным примером информационной войны считается Холодная война 1946–1991 годов (точнее, её идеологический аспект). Многие исследователи полагают, что распад СССР был обусловлен именно применением информационных методов, что наиболее активной части населения были навязаны установки, которые и запустили внутренние политические процессы, закончившиеся Перестройкой и распадом.

С распадом СССР информационная война не прекратилась, а наоборот усилилась, потому, как Россия осталась правопреемником СССР и все еще вызывает опасения запада. В настоящее время ведется скрытая и, нередко даже явная, пропаганда чуждых русскому и другим братским народам идей, посредством подконтрольных мировому капиталу СМИ, таких как телевидение, радио и печатные издания, где вместо общечеловеческих ценностей в людях культивируются низменные пороки, отсутствие уважения друг к другу, к своей Родине и к родителям. Воспевается культ денег.

На сегодняшний день **информационная война** – это форма борьбы сторон, представляющая собой использование специальных (политических, экономических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Информационные войны имеют множество значений и определений, в зависимости от среды действия, и развития новых технологий.

Вместе с тем становление информационного общества создает предпосылки информационных катастроф. Это могут быть катастрофы технические, связанные с неполадками в ИС и программах, но это могут быть и катастрофы гуманитарные, связанные с разрушением нравственного и социального мировоззрения, обеспечивающего гармоничное развитие общества.

Сейчас имеется множество определений информационной войны. Так автор работы «Что такое информационная война?» Мартин Либики определил семь разновидностей информационной войны (командно-управленческая, разведывательная, психологическая, хакерская, экономическая, электронная и кибервойна).

- **Командно-управленческая война** в качестве основного объекта воздействия рассматривает каналы связи между командованием и исполнителями. Перерезая «шею» (канал связи), нападающий изолирует «голову» от «туловища». Считается, что Интернет родился как оборонный вариант этой войны.
- **Разведывательная война** имеет целью сбор важной в военном отношении

информации и защиту собственной.

- **Электронная война** объектом своего воздействия имеет средства электронных коммуникаций – радиосвязи, радаров и компьютерных сетей. Ее важная составляющая –криптография, позволяющая осуществлять шифрование и расшифрование электронной информации.

- **Психологическая война** – осуществляется путем пропаганды, «промывания мозгов» и другими методами информационной обработки населения.

М. Либики выделяет **четыре составляющие психологической войны** (подрыв гражданского духа; деморализация вооруженных сил; дезориентация командования; война культур).

- **Хакерская война** имеет целями тотальный паралич сетей, перебои связи, введение ошибок в пересылку данных, хищение информации, хищение услуг за счет несанкционированных подключений к сетям, их тайный мониторинг, несанкционированный доступ к закрытым данным. Для достижения этих целей используются различные программные средства: вирусы, «логические бомбы», сниферы («нюхалки», «следилки») и др..

- **Экономическая информационная война.** М.Либики выделяет две ее формы: информационную блокаду (направленную против США) и информационный империализм (метод самих США).

Мир продолжает стремительно изменяться и ставит множество новых вопросов перед человечеством. Революционные изменения видны во многих отраслях мировой экономики, в первую очередь, область информатизации общества. Волна «цифровой революции» создала абсолютно новый экономический сектор, которого раньше просто не было.

Основной продукт этого сектора – информация, обладающая уникальными свойствами. Информация, в отличие от всех других ресурсов, пригодна для многократного использования и для многочисленных пользователей, при этом, чем больше она применяется, тем более ценной становится.

2. Субъекты информационного противоборства

К ним относят: государства, их союзы и коалиции; международные организации; негосударственные незаконные (в том числе — незаконные международные) вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности; транснациональные корпорации; виртуальные социальные сообщества; медиа-корпорации (контролирующие средства массовой информации и массовой коммуникации — СМИ и МК); виртуальные коалиции.

Остановимся более подробно на характеристике основных субъектов информационного противоборства:

- Государства, их союзы и коалиции. Этот вид субъектов информационного противоборства имеет, как правило, стабильные (постоянные) интересы в информационном пространстве; формирует и контролирует национальное (союзное) информационное пространство, которое, как правило, так или иначе интегрировано в глобальное информационное пространство и является его сегментом; создает как в силовом блоке, так и в гражданских государственных учреждениях специальные силы и структурные подразделения, в функции и задачи которых входит ведение информационного противоборства; при наличии необходимого научно-технического потенциала разрабатывает и испытывает системы информационного оружия, средств его доставки и маскировки, а также принципы боевого применения; в случае, когда собственный научно-технический потенциал не позволяет осуществлять подобные разработки, приобретает (легально или тайно) эти средства за рубежом.

- Международные организации. Этот вид субъектов информационного противоборства: имеет, как правило, стабильные (постоянные) интересы в информационном пространстве; участвует в формировании глобального информационного пространства и частично контролирует национальные сегменты информационного пространства; создает в рамках своих структур или использует национальные структуры, интегрированные в международные организации, в функции которых входит информационное противоборство.

- Негосударственные незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности. Этот вид субъектов информационного противоборства: имеет интересы в информационном пространстве; создает собственный (часто - закрытый) сегмент информационного пространства, стремится к захвату или контролю (а также к разрушению и замещению на собственный) сегментов национального и/или глобального информационного пространства; создает в рамках своих или союзных структур силы, в функции и задачи которых входит ведение информационного противоборства.

- Транснациональные корпорации. Этот вид субъектов информационного противоборства обладает теми же характеристиками (признаками), что и международные организации: имеет, как правило, стабильные (постоянные) интересы в информационно-телекоммуникационном пространстве;

участвует в формировании глобального информационного пространства и частично контролирует национальные сегменты информационного пространства; создает в рамках своих структур или использует национальные структуры государств, интегрированных в контролируемое данным субъектом информационное и телекоммуникационное пространство, в функции и задачи которых входит ведение информационного противоборства; создает и использует собственный научно-технический потенциал и/или использует (стимулирует создание) потенциал стран, так или иначе интегрированных в сегмент информационного пространства, принадлежащего и/или контролируемого корпорацией, или принимающих участие в ее деятельности, для разработки и испытаний образцов и систем информационного оружия, средств его доставки и маскировки, принципов применения, а также приобретает при необходимости (тайно) данные средства у третьей стороны; разрабатывает и закрепляет на официальном уровне, в том числе в виде ведомственных нормативных актов, концептуальные и идеологические положения, обосновывающие необходимость участия в информационном противоборстве, определяющие основные принципы и формы участия в нем для данного субъекта. Особую роль в информационной борьбе владельцев открытых информационно-телекоммуникационных сетей (ОТКС) и разработчиков сетевых технологий — сетевых информационных корпораций и корпораций-провайдеров, обеспечивающих циркуляцию жизненно важных потоков информации, можно охарактеризовать следующим образом. **В информационном обществе условия диктует тот, в чьих руках находятся информационные сети, ресурсы и технологии.** Контроль за сетевыми ресурсами сосредоточен в руках провайдеров, обеспечивающих доступ в открытые телекоммуникационные сети для других компаний, организаций и частных лиц и гарантирующих стабильность работы с информацией. Деятельность провайдеров может подвергаться контролю и давлению как со стороны фирм и корпораций, так и органов власти тех государств, на территории которых находятся их серверы, представительства, активы.

Таким образом, компании, контролирующие информационные потоки, все больше приобретают черты транснациональных государств-корпораций, интересы которых лежат на территориях различных стран с различными законами, традициями, геополитическим положением и государственным устройством. Можно прийти и к выводу о том, что в ближайшем будущем в любом вооруженном конфликте будут задействованы силы и средства как ми-

нимум трех сторон — агрессора, жертвы и (одной или нескольких) корпораций.

4. Составные части и методы информационного противоборства

Следует различать информационное противоборство (борьбу) в широком (во всех сферах) и узком смысле слова (в какой-либо сфере, например, в политической сфере). **Информационное противоборство** (борьба) –форма борьбы сторон, представляющая собой использование специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Основные сферы ведения информационного противоборства: • политическая; • дипломатическая; • финансово-экономическая; • инновационная; • военная.

Следует выделить **два вида информационного противоборства** (борьбы): информационно-техническое и информационно-психологическое.

При информационно-техническом противоборстве главными объектами воздействия и защиты являются информационно-технические системы (системы связи, телекоммуникационные системы, системы передачи данных, радиоэлектронные средства, системы защиты информации и т. д.).

При информационно-психологическом противоборстве главными объектами воздействия и защиты являются психика политической элиты и населения противостоящих сторон; системы формирования общественного сознания и мнения, принятия решений.

Информационное противоборство (в политической сфере) включает **три составные части:** – стратегический политический анализ; – информационное воздействие; – информационное противодействие.

Стратегический политический анализ – это комплекс мероприятий по добыванию информации о противнике (конкуренте) и условиях информационного противоборства; сбору информации о своих союзниках; обработке информации и обмену ею между членами своего политического содружества в целях организации и ведения действий.

Информационное воздействие. Оно включает мероприятия по блокированию добывания, обработки и обмена информацией, дезинформации.

Информационного противодействие (защита), включает действия по деблокированию информации, необходимой для решения задач управления политическими процессами, и блокирования дезинформации, распространяемой и внедряемой в систему формирования общественного мнения.

Уровни ведения информационного противоборства: • стратегический; • оперативный; • тактический.

В основном, на стратегическом уровне информационного геополитического противоборства должны действовать высшие органы государственной власти России, а спецслужбы и крупный национальный капитал – на оперативном и тактическом уровнях.

Ведущие страны мира в настоящее время располагают мощным информационным потенциалом (прежде всего США, Китай, Великобритания), который может обеспечить им достижение глобальных политических и экономических целей, тем более что отсутствуют международные юридические нормы ведения информационной войны.

Необходимо также определить содержание понятия «воздействие».

Воздействие – действие, направленное на кого-нибудь с целью добиться чего-нибудь, внушить что-нибудь.

В психологии под воздействием понимается целенаправленный перенос информации от одного участника взаимодействия к другому. Воздействие может быть непосредственное (контактное) и опосредованное (дистанционное, с помощью чего-либо). Именно воздействие является целью производства информации. Если же говорить о социальных объектах, то к ним можно отнести отдельных индивидов, социальные группы, общество, государство, мировое сообщество. Основными социальными элементами общества являются социальные группы и отдельные индивиды.

Для защиты от негативных воздействий социальных объектов в ходе глобального геополитического информационного противоборства, необходимо создание системы информационно-психологического обеспечения как составной части национальной безопасности России. Данная система должна обеспечить защиту психики политической элиты и населения России от негативного информационно-психологического воздействия (т. е. защите СОЗНАНИЯ россиян от негативных информационных потоков противников России). Ее основная задача – обеспечение психологической безопасности политической элиты и населения России.

Информационно-психологическое воздействие представляет собой целенаправленное производство и распространение информации, оказывающей непосредственное влияние (положительное или отрицательное), на функционирование и развитие информационно-психологической среды общества, психику и поведение политической элиты и населения России.

В связи с появлением и ускоренным развитием СМИ резко усилилась роль общественного мнения, которое стало влиять колоссальным образом на политические процессы в обществе, особенности функционирования информационно-психологической среды общества. Поэтому система формирования общественного мнения также является одним из основных объектов информационно-психологического обеспечения. Следовательно, необходимо изучение особенностей формирования и функционирования общественного мнения при вооруженных конфликтах, на основе которого следует выработать практические пути обеспечения психологической безопасности политической элиты и населения России.

Информационное оружие – это устройства и средства, предназначенные, для нанесения противоборствующей стороне максимального урона в ходе информационной борьбы (путем опасных информационных воздействий).

Объектами воздействия могут являться: - информационно-технические системы; - информационно-аналитические системы; - информационно-технические и информационно-аналитические системы, включающие человека; -информационные ресурсы; - системы формирования общественного сознания и мнения, базирующиеся на СМИ и пропаганды; - психика человека.

Методы применения информационного оружия: нанесение ущерба отдельным физическим элементам информационной инфраструктуры (разрушение сетей электропитания, создание помех, использование специальных программ, стимулирующих вывод из строя аппаратных средств, а также биологических и химических средств разрушения элементарной базы); уничтожение или повреждение информационных, программных и технических ресурсов противника, преодоление систем защиты, внедрение вирусов, программных закладок и логических бомб; воздействие на ПО и базы данных информационных систем и систем управления с целью их искажения или модификации; угроза или проведение террористических актов в информационном пространстве (раскрытие и угроза обнародования или обнародование конфиденциальной информации об элементах национальной информационной инфраструктуры, общественно значимых и военных кодов шифрования, принципов работы систем шифрования, успешного опыта ведения информационного терроризма и др.); захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации силы и доведения своих требований; уничтожение и подавление линий связи, искусственная перегрузка узлов

коммутации; воздействие на операторов информационных и телекоммуникационных систем с использованием мультимедийных и программных средств для ввода информации в подсознание или ухудшения здоровья человека; воздействие на компьютеры боевой техники и вооружений с целью вывода их из строя.

Таким образом, создание единого глобального информационного пространства, являющееся естественным результатом развития мировой научно-технической мысли и совершенствования информационных технологий, создает предпосылки к разработке и применению информационного оружия.

Владение эффективным информационным оружием и средствами защиты от него становится одним из главных условий обеспечения национальной безопасности государства в XXI веке.

Контрольные вопросы

1. Определение информационно-психологического воздействия. Примеры.
2. Раскрыть сущность понятия «информационная война».
3. Пояснить суть составляющих психологической войны.
4. Назвать основные средства Хакерской войны.
5. Основные субъекты информационного противоборства.
6. Назвать основные сферы ведения информационного противоборства.
7. Составные части информационного противоборства в политической сфере.
8. Пояснить сущность уровней ведения информационного противоборства.
9. Что понимается под информационно-психологическим воздействием.
10. Информационное оружие и основные методы его применения.

ТЕМА 6. ПРИЕМЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ В ИНФОРМАЦИОННОЙ ВОЙНЕ

1. Информационная война как целенаправленное информационное воздействие информационных систем

2. Способы перепрограммирования информационных систем

3. Проблема начала информационной войны

Литература:

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. - 392с.

2. Малюк А.А. Защита информации в информационном обществе. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2015. – 230 с.

3. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 с.

Многие приемы информационного воздействия возникли тысячи лет назад вместе с появлением информационных самообучающихся систем.

При этом вполне естественно, что с повышением способностей ИС в части их обучения акцент будет все более и более смещаться в сторону применения не огнестрельного оружия, а информационного: если систему дешевле уничтожить и создать заново в нужном виде, чем переучить, то ее уничтожают, если же ее проще переучить, то переучивают. Выйти победителем в информационной войне — это значит вовремя понять, чему можно обучаться, а чему нельзя, т.е. какие входные данные можно обрабатывать, а какие — ни в коем случае.

1. Информационная война как целенаправленное информационное воздействие информационных систем

Под системой могут пониматься: человек, компьютер, природный ландшафт и др. Разница между этими системами в том, что если для тех из них, которые принято называть информационными, модификация внутренних управляющих структур связана с получением новой информации, с обучением, то модификации механических или природных геобразований, с нашей, человеческой точки зрения, носит несколько иной характер.

Горный обвал может изменить течение реки, засыпав ее камнем и песком, а для того, чтобы изменить поведение человека или животного, достаточно показать им этот обвал; чтобы откорректировать горную цепь, требуется землетрясение, а для изменения поведения жителей достаточно и информации о грядущем землетрясении. Чем полнее система воспринимает внешний мир, тем более «тонкими» энергиями можно воздействовать на ее поведение.

Можно ли определить понятие «информационной системы», не прибегая к термину «информация»? Вот именно об этом дальше и пойдет речь.

Информационная система — это система, осуществляющая: получение входных данных; обработку этих данных и/или изменение собственного внутреннего состояния (внутренних связей/ отношений); выдачу результата либо изменение своего внешнего состояния (внешних связей/отношений).

Нарушение защитных барьеров во взаимодействии элементов сложной системы друг с другом приводит к перепрограммированию этих элементов и/или их уничтожению. Из сказанного следует, что информационным "полем боя" являются в первую очередь протоколы информационно-логического сопряжения элементов сложной системы, средства и технологии их практической реализации.

Протокол информационно-логического взаимодействия для элементов социального пространства нашел свое воплощение в естественном языке каждого народа. Использование того или иного языкового подмножества языка во многом определяет информационные возможности различных групп населения. Основными средствами корректировки протоколов информационно-логического взаимодействия для социального пространства сегодня стали СМИ. Протокол информационно-логического взаимодействия для элементов кибернетического пространства отражен во множестве языков программирования, в сетевых протоколах. Основными средствами корректировки этих протоколов являются программные закладки, компьютерные вирусы, а также всевозможные технические средства и технологии воздействия на каналы телекоммуникаций.

Теперь настало время дать определение понятию информационной войны: **информационная война между двумя информационными системами — это открытые и скрытые целенаправленные информационные воздействия (ИВ) систем друг на друга с целью получения определенного выигрыша в материальной сфере.**

Информационное воздействие осуществляется с применением информационного оружия, т.е. таких средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия. Для технических систем самый простой пример выглядит следующим образом. Компьютерная программа получает на вход значения двух переменных и делит первое на второе. Понятно, что если злоумышленник или сама жизнь подсунет в качестве значения второй переменной ноль, то результат может быть самым неожиданным, что при определенных условиях приведет к гибели и всей ранее накопленной информации.

Системы целенаправленного сбора информации и контроля за объектами в режиме реального времени выводятся из строя путем создания перегрузок, например: «Космическая техника, особенно базирующаяся на геостационарной орбите, совершенно не является ремонтнопригодной, не может быть оперативно заменена и очень уязвима к воздействию современных средств радиоэлектронного подавления (РЭП). Дело в том, что приемные устройства связных и разведывательных спутников выполнены очень чувствительными (детекторы «Магнум» засекают сигналы, начиная с 10 в минус четырнадцатой степени Вт) и защищены только от помех или перегрузок, сравнимых по длительности с продолжительностью полезных сигналов. Ме-

гаваттное воздействие с поверхности Земли, произведенное средствами РЭП на нужной частоте, неизбежно приведет к потере приемного устройства спутника, а, следовательно к выводу из строя всего канала связи».

Для более сложной информационной системы, например, такой, как человек, ИВ, способное вывести из строя систему, это прежде всего активизация таких желаний, мыслей и провоцирование поступков, направленных на саморазрушение.

Под войной информационных систем будем понимать их действия, направленные на получение материального преимущества, путем нанесения противнику ущерба, с помощью соответствующего ИВ.

В данном случае предполагается, что пока противник устраняет полученный ущерб, т.е. занят только собой, противная сторона имеет преимущество во внешнем мире. Понятно, что подобная война имеет смысл лишь для систем, потребляющих для своей жизнедеятельности общие ограниченные материальные ресурсы.

2. Способы перепрограммирования информационных систем

Дадим несколько неформальных определений:

а) две информационные обучающиеся системы (ИОБ системы) называются «понимающими» друг друга, если на абсолютное большинство одинаковых входных сообщений, они выдают одинаковые по смыслу результаты;

б) две ИОБ системы называются «похожими» друг на друга, если на абсолютное большинство одинаковых входных сообщений, они выдают одинаковые по форме результаты;

в) две ИОБ системы называются «агрессивными» друг для друга, если имеет место «похожесть» между ними, но полностью отсутствует «понимание»; более того, «понимание» вообще стремится к нулю.

«Понимающее», «похожее» или «агрессивное» поведение таких информационных систем, как люди, находит свое отражение как на бытовом уровне, так и на религиозном, и государственном. При одном и том же входном сообщении один человек ложится отдыхать под пальму, другой начинает считать возможные прибыли, третий сочиняет научный трактат.

Утверждение 1. Для того чтобы информационная самообучающаяся система способна была целенаправленно перепрограммировать другую подобную систему, она должна ее «понимать». Примером служит цель перепрограммирования в мире ПО для «народа»: «Многие были свидетелями, но уже мало кто вспоминает о том, что заря Windows занялась во второй поло-

вине 1992 года с беспрецедентного кругосветного пропагандистского турне руководства Microsoft с массой речей и выступлений на сотнях бизнес-встречах, семинарах и международных выставках. Главной целью этой акции было всколыхнуть мировую общественность, увлечь за собой и привязать к себе ведущих мировых производителей, которые после переориентации своих перспективных разработок (и связанных с этим капиталовложений) уже не смогут «Уклониться от магистрального пути». А уж за ними поплетутся массы пользователей, быстро привыкающие считать такой мир единственным. Этот замечательный пример показал всем сообразительным, что затраты на рекламу значительно эффективнее, чем затраты на корпоративное «дорабатывание» продуктов. Поэтому с приходом Windows началась резкая деградация качества ПО и его усложнение. Тем самым несомненной заслугой Б. Гейтса является открытие и наглядная демонстрация сверхмощных механизмов массового порабощения в эру информационной цивилизации».

Следствие: подобрать входные данные для системы в соответствии с заданной целью перепрограммирования— это значит заставить ИС «смотреть на мир чужими глазами», глазами той информационной системы, на которую данная система должна стать похожей, т.е. глазами эталона. Способна ли ИС защититься, если враг применит против нее описанный способ перепрограммирования ИС? Безусловно. Для этого достаточно «закрыть глаза» на те входные данные, которые подаются на вход противной стороной. Причем, во многих странах данный способ защиты населения закреплен законодательно.

«Даже в 70-е годы, когда Америка увязла в войне во Вьетнаме, американские СМИ, критикуя эту войну, «торпедируя» ее, не позволяли себе использовать съемки телеоператоров, работавших со стороны Вьетнама. Более того, в той же Америке, а также Англии, Франции и еще десятке стран существует строжайший законодательный запрет на использование любых кино-, фото; видео и печатных материалов, снятых или написанных на стороне тех, кто ведет боевые действия против армий этих стран, и даже просто имеющих сочувственные «врагам» интонации или же идеи»

В.Шурыгин, анализируя информационный аспект военных действий в Чечне, подробно описывает, как был реализован способ перепрограммирования информационной системы на практике: «В среднем чеченская тематика занимала в программах НТВ от 10 до 18 минут на информационный выпуск, в «Вестях» (информационная программа российского телевидения) от 3 до 7 минут. Так вот, у НТВ до 80% всех видеосъемок непосредственно боевых действий велось со стороны чеченских боевиков или использовались пленки,

снятые со стороны сепаратистов. В «Вестях» это соотношение достигало 60%. Оставшиеся 20% НТВ обычно делило между съемками разрушений, обычно приписываемых армии, интервьюировании местных жителей-чеченцев, «страдающих от русской агрессии», или же комментариями своих тележурналистов, в лучшем случае на фоне российских позиций, но чаще у сгоревшей российской техники. Так же примерно делили оставшийся эфир и «Вести».

Анализ публикаций таких газет, как «Московский комсомолец» и «Известий», выявил следующее: лишь в одной из четырех статей упоминалась или раскрывалась точка зрения на происходящие события федерального командования. Три же из четырех публикаций носили или же откровенно проченческий характер, героизируя боевиков, преувеличивая их возможности, или же жестко критиковали армию и ее действия в Чечне».

Опросы общественного мнения, проводимые НТВ, возможно, с целью проверки эффективности данного способа перепрограммирования, подтверждали, что для среднестатистического гражданина, регулярно смотрящего телевизор, отношение к собственной армии изменяется в худшую сторону, а цели боевиков становятся «ближе и понятнее».

Все виды ИВ на информационную систему можно попробовать классифицировать еще и следующим образом: 1) входные данные — «сухие» факты;

2) входные данные — логически обоснованные выводы; 3) входные данные — эмоционально окрашенные утверждения. Эмоции, являясь критерием истинности в процессе познания, могут быть присущи только самообучающейся ИС, как способ внешнего проявления усвоенного знания.

При этом эмоциональный заряд для любой входной последовательности повышает скорость ее обработки информационной системой, порой минуя даже обязательные логические проверки. Например, эмоционально насыщенный крик о помощи или об опасности заставляет сразу же совершать определенные действия и уже только потом, если будет возможность, проверять логикой возможность тех или иных утверждений.

Утверждение 2. «Понимающие» ИС формируются одинаковыми эмоциональными воздействиями, как правило, минуя средства защиты, основанные на логике. Например, диктор телевидения монотонно сообщает факты о поездках по стране кандидатов в президенты. При этом, не искажая факты, говоря об одном из них, он подкрепляет свои слова мимикой, выражающей презрение, а в случае упоминания другого кандидата, наоборот, вся его фи-

зиономия сияет от счастья. В результате у зрителей скрытно от них самих начинает формироваться соответствующее отношение к кандидатам. Видно, что в данном случае сама возможность сказать что-то (даже совсем нейтральное) о том или ином кандидате может использоваться для перепрограммирования нечаянных слушателей. Аналогичным образом формируются информационные материалы в прессе. Текст сообщения содержит «голые» факты, к которым не может быть претензий, а название заметки, особенно если речь идет о конкурентах, имеет обязательную эмоциональную окраску. Сообщение прочитают не все, но на заголовок обязательно обратят внимание, а тем самым неявно свяжут возникшее эмоциональное ощущение с объектом газетного материала.

Следствие: для перепрограммирования самообучающихся ИС, обладающих эмоциями, наиболее эффективным средством является «эмоционально окрашенная» входная обучающая последовательность. В случае быстрого и массового перепрограммирования народа, нации наиболее эффективными являются приемы, имеющие эмоциональную окраску и принадлежащие таким сферам как: массовые культура, искусство, религия.

Это значит, что для решения задач по перепрограммированию населения в первую очередь упор должен делаться на деятелей искусства, культуры, религиозных служителей.

Утверждение 3. Разрушение устоявшихся структур, приведение их в хаотическое состояние способствуют повышению избыточности хаоса, а тем самым увеличению возможностей для перепрограммирования систем.

Следствие: для эффективного перепрограммирования устоявшихся структур необходимо предварительно привести их в хаотическое состояние путем разрушения устоявшихся связей и уничтожения наиболее значимых базовых элементов.

Утверждение 4. Для любой ИС безопасно оперировать с той информацией, механизмы обработки которой уже существуют у данной системы. Сказанное достаточно просто объясняется на уровне здравого смысла. Для технической системы, согласно утверждению 4, безопасными входными данными являются те, которые уже были у нее в прошлом, которые принадлежат множеству допустимых входных/выходных значений. Для социальных и биологических систем — это функционирование в рамках привитых привычек, сложившегося образа жизни, сформированных стереотипов поведения в условиях известного (предсказуемого) системе внешнего окружения.

Следствие: в любое время наиболее безопасно транслировать на свое окружение информацию о достоинствах собственного образа жизни (примеры западного образа жизни).

Сложившиеся стереотипы поведения — это то пространство действий, в котором конкретная система наиболее эффективно способна противостоять внешним, известным системе угрозам.

Естественно, что для каждой системы именно ее собственные привычки и являются ее достоинством. Они во многом определяют данную систему, так как обеспечивали и обеспечивают ее существование. Навязывание собственных стереотипов поведения окружающим системам, особенно уже сформированным неизбежно будет ослаблять последних. Это объяснимо — всегда тяжело играть на чужом поле, да еще по неизвестным правилам.

Таким образом, наличие в поведении системы приемов, в основе которых лежат приведенные выше утверждения и следствия, является одним из признаков информационного нападения.

3. Проблема начала информационной войны

Одним из ключевых вопросов, выводящих на неразрешимость проблемы выигрыша в информационной войне, заключается в следующем: «Способна ли ИС определить, что против нее начата информационная война?».

Пусть существуют две противоборствующие информационные системы - ИС1 и ИС2, системы защиты у которых функционально похожи и работают по следующему алгоритму: 1) получение входной информации; 2) анализ входной информации в течение времени t: - определение источника информации; - определение целей информатора; - оценка правдоподобности, если поступившая информация оценена как факт агрессии, то - к п. 3, иначе, к п. 1;

3) выдача на вход агрессора адекватной информации, что подразумевает ответный удар, т.е. информационную войну.

Теперь посмотрим, что может произойти при взаимодействии подобных систем. У этого простого алгоритма оказывается достаточное большое число вариантов развития: 1) ИС1 оценила неопасную информацию как факт агрессии и применила ответные меры; 2) ИС1 оценила начало войны как неопасную информацию и соответственно проиграла войну; 3) ИС1 не успела оценить информацию за время, которого достаточно для адекватного реагирования, и в этом случае она либо не пострадала, если информация действительно неопасная, либо проиграла.

Предположим, что обе системы не желают выступать в роли агрессора. Тогда для любой из них главной задачей является идентификация сигналов, поступающих на вход, именно от системы защиты противной стороны. И задача сводится к следующему: 1) если входная инф. поступила на вход ИС1 от системы защиты ИС2, то это означает начало войны; 2) если входная инф. поступила на вход ИС2 от системы защиты ИС1 то это означает начало войны.

По сути дела, мы рассматриваем ситуацию о применимости любого из названных алгоритмов к самому себе (в силу их функциональной идентичности). Получилось, что в общем случае задача любой из ИС заключается в том, чтобы понять - результат работы какого алгоритма она исследует, т.е. какой алгоритм она исследует, алгоритм ли вообще подан на вход?

В этой ситуации грозить адекватным ответом, например в виде «термоядерной дубины», бессмысленно, так как объективно невозможно доказать факт информационной атаки.

Получается, что начало информационной войны определить невозможно, и это дает определенные преимущества агрессору. Но парадокс заключается в том, что если жертва нападения успеет осознать, что против нее ведется информационная война, то полученное агрессором преимущество на начальном этапе, в подобного типа войнах, совсем не коррелирует с мелодией гимна победителя. В реальной жизни так оно и бывает. Дождь за окном намекает на необходимость взять зонт, выходя на улицу. Футбольный мяч, закатившийся на тротуар, требует удара по себе. Автобус, неожиданно подъехавший к остановке, когда уже принято решение никуда не ходить и вернуться домой, отменяет это решение.

Важно, что эти «вещи» заставляют систему выйти из состояния, в котором ее поведение практически не предсказуемо, и перейти к выполнению того сценария, который навязывается «этими вещами». Действительно, как можно не ударить по мячу, когда он выкатился под ноги?

Хорошо продуманная последовательность подобных «вещей» и образует ту обучающую выборку, с помощью которой осуществляется целенаправленное управление информационной системой.

Таким образом, государству необходимо уметь определять момент начала информационной войны и всегда иметь заготовленный алгоритм ответных действий.

Контрольные вопросы

1. Привести примеры информационных воздействий.

2. Раскрыть понятие перепрограммирования информационных систем.
3. Привести примеры открытых и скрытых целенаправленных информационные воздействий систем друг на друга.
4. Примеры перепрограммирования людей в мире ПО.
5. Сущность формальных определений информационных обучающихся систем.
6. Каким образом можно перепрограммировать информационную систему?
7. Способы перепрограммирования ИС с использованием СМИ.
8. Способы защиты от перепрограммирования информационной системы.
9. Алгоритм защиты от перепрограммирования информационной системы.
10. Зачем нужно знать время начала информационной войны?

ТЕМА 7. ТИПОВАЯ СТРАТЕГИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ

1. Обобщенный алгоритм информационной войны

2. Основные аспекты информационной войны

3. Последствия информационной войны

Литература:

1. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 С.

1. Обобщенный алгоритм информационной войны

Любая ИОБ система обладает базовым набором смыслов или знаний, который во многом и определяет поведение этой системы. Существование базового набора обеспечивается физическими носителями— соответствующими структурами в рамках общей структуры и/или соответствующими отдельными элементами, которые в дальнейшем будем называть базовыми элементами.

Понятно, что в зависимости от количества базовых элементов и их связей противная сторона (система-агрессор) либо способна, используя собственные научно-технические достижения, в короткие сроки промоделировать поведение базовых элементов, либо нет. В том случае, если моделирование возможно, будем считать, что базовые элементы системы X моделируются системой Y. Отсюда следует, что, так как у каждой ИС в зависимости от ее собственной структуры количество базовых элементов и их связей различно, то у одной системы базовые элементы являются моделируемыми ее врагом в ходе подготовки или ведения информационной войны, а у другой нет. Например, если речь идет об иерархически упорядоченных самообучаемых структурах, базовые элементы, определяющие систему, можно пересчитать по пальцам - их немного. Поэтому становится возможным в отпущенное ис-

следователю (или противнику) время проектировать, моделировать и реализовывать любые алгоритмы информационного воздействия.

При этом, безусловно, определяющими факторами при разработке средств информационного оружия становятся именно индивидуальные особенности элементов. Для того чтобы смоделировать поведение базовых элементов, необходимо знать индивидуальные особенности и предпочтения.

Утверждение. Чем больше мощность множества базовых элементов и их связей, тем система устойчивее к целенаправленному ИВ.

Что может собой представлять конкретный алгоритм информационной войны с конкретным противником? Подобный алгоритм описан философом А. Зиновьевым на примере информационной войны Запада с Советским Союзом.

1. Для изучения индивидуальных особенностей и потенциальных возможностей «базовых элементов» СССР на Западе была создана целая наука со своими служителями - Кремлинология.

2. «Кремлинологи самым дотошным образом изучали аппарат ЦК. И не только изучали, а оказывали на партийных руководителей влияние. Как? Через СМИ. Через помощников, советников. Через дипломатов, журналистов, агентов. Можно признать, как факт, что Запад в восьмидесятые годы начал во все усиливающейся степени манипулировать высшим советским руководством.»

3. «Кремлинологи изучили ситуацию еще при Брежневе... . Андропов и Черненко были больны, долго протянуть не могли. Так что главную роль так или иначе предстояло сыграть кому-то из двух — Романову или Горбачеву. Изучив досконально качества того и другого (а возможно, уже как-то «подцепив на крючок» Горбачева ранее), в соответствующих службах Запада решили устранить Романова и расчистить путь Горбачеву».

4. «В средствах массовой информации была изобретена и пущена в ход клевета на Романова (будто он на свадьбу дочери приказал принести драгоценный сервиз из Зимнего дворца), и началась его всяческая дискредитация. Причем, изобретатели клеветы были уверены, что «соратники» Романова его не защитят. Так оно и случилось. Даже Андропов, считавшийся другом Романова, не принял мер, чтобы опровергнуть клевету. Мол, не стоит на такой пустяк реагировать. А между тем это был не пустяк, а начало крупномасштабной операции с далеко идущими последствиями».

5. «Возьмите теперь сами выборы Генсека! В том, что они были явно частью операции соответствующих служб США, даже на Западе многие хорошо понимали. Все было подстроено умышленно так, что выбирало всего 8 человек.

Задержали под каким-то предлогом вылет из США члена Политбюро Щербицкого, который проголосовал бы против Горбачева. Не сообщили о выборах другому члену Политбюро, находившемуся в отпуску. Это был сам Романов, который тоже наверняка проголосовал бы против Горбачева. Если бы хотя бы эти двое голосовали, Горбачев не стал бы Генсеком (перевес в один голос)!

Причем, подобный алгоритм целенаправленного информационного воздействия, был изложен почти сто лет назад в документе под названием «Протоколы собраний Сионских мудрецов».

2. Основные аспекты информационной войны

Не вдаваясь в споры о причинах и источнике данного документа, хотелось бы отметить, что его авторов бесспорно следует назвать первыми серьезными теоретиками в области построения типовых тактик и стратегий ведения информационных войн. В названном документе можно прочитать следующее: «Чтобы привести наш план к такому результату, мы будем подстраивать выборы таких президентов, у которых в прошлом есть какое-нибудь нераскрытое темное дело, какая-нибудь «панама» — тогда они будут верными исполнителями наших предписаний из боязни разоблачений и из свойственного всякому человеку, достигшему власти, стремления удержать за собою привилегии, преимущества и почет, связанный со званием президента» (Протокол 10). «В руках современных государств имеется великая сила, создающая движение мысли в народе — это пресса» (Протокол 2). «Ни одно оповещение не будет проникать в общество без нашего контроля. Это и теперь уже нами достигается тем, что все новости получаются несколькими агентствами, в которых они централизуются со всех концов света. Эти агентства будут тогда уже всецело нашими учреждениями и будут оглашать только то, что мы им предпишем.

Кратко и точно в "Протоколах ..." сказано практически обо всех аспектах информационной войны: - система управления (контроль властных структур); - средства перепрограммирования населения (СМИ); - терроризм; - экономические войны; - средства экономического управления; - финансовая программа; - всеобщее голосование и т.д.

Данные протоколы носят методический характер. Они составлены так, что их может использовать любой, понимающий значимость тайной войны, и совсем не обязательно ограничивать их применение только мудрецами и только тем далеким временем. С точки зрения значимости для теории информационной войны данные протоколы, наверное, в чем-то аналогичны

первым робким исследования по теории ядерного оружия, кстати, относящимся примерно к тому же времени. Сионские протоколы» поучительны тем, что дают канву и рисунки, по которым действительно вышивается саморазложение христианской культуры. В труде нет математических формул и доказанных теорем, но есть простое и доступное обоснование: должно быть именно так, а не по-другому. Оппонент может возразить: А при чем здесь наука? При чем здесь вообще информационная война и «западизация»? То, о чем пишет А.Зиновьев, - это обычные методы борьбы, известные со времен царей, королей и шахов; суть их — посадить на трон своего человека.

Теперь о так называемом «побеждающем» алгоритме. Тексты А. Зиновьева ничего не говорят об его универсальности. Да, описанный алгоритм существовал века. Что же изменилось? Изменились многие методы и приемы, они получили научное обоснование. Возникли целые научные дисциплины о том, как управлять поведением человека, коллектива, общества. К ним относятся: социология, психоанализ, теория рекламы, суггестология, NLP-программирование, дианетика и т.п.

Получил свое теоретическое обоснование гипноз и были сделаны попытки перенесения методов гипнотического воздействия с отдельного индивидуума на коллективы и на целые человеческие общества. Всего этого еще не было даже в прошлом веке — не было достаточно эффективных средств массовой информации, не было научно обоснованных алгоритмов управления социумом; а возникнуть эти алгоритмы могли только с появлением теории программирования для сегодняшних средств вычислительной техники.

Информационное оружие — это прежде всего алгоритм. Применить информационное оружие — это значит так подобрать входные данные для системы, чтобы активизировать в ней определенные алгоритмы, а в случае их отсутствия активизировать алгоритмы генерации нужных алгоритмов.

Имеющаяся на сегодняшний день теория алгоритмов позволяет объяснить, каким образом может осуществляться автоматическое написание программ для определенных предметных областей.

Например, можно, взяв за основу работу Ч. Тарта «Состояния сознания», попробовать по аналогии перенести методы гипнотического внушения с индивидуума на коллектив. Наведение гипнотического состояния на отдельного индивидуума у Ч.Тарта описывается в виде алгоритма так: 1) расслабить тело (цель данного действия: организм как целое должен исчезнуть в качестве объекта сознания); 2) слушать только гипнотизера, не обращая внимания на какие-то иные мысли или ощущения (цель: процесс нагружения

сознания и действие формирующих сил ослабляются); 3) не размышлять над тем, что говорит гипнотизер (цель: способствует торможению непрерывного потока мыслей); 4) сосредоточить внимание на каком-то предмете помимо голоса самого гипнотизера (цель: подсистема сознания, ответственная за обработку чувственной информации, оказывается не в состоянии выполнять свою функцию и как бы расстраивается); 5) гипнотизер внушает, что вы спите или засыпаете (цель: внушение сна ослабляет память и чувство самоотождествленности, которыми характеризуется состояние бодрствования); 6) гипнотизер убеждает человека, что этот сон не совсем настоящий сон (цель: создание пассивного, подобного сну состояния сознания, в котором сохраняется возможность контакта с гипнотизером).

По аналогии процесс наведения гипнотического состояния на отдельное общество мог бы, наверное, выглядеть следующим образом: 1) расслабить общество — внушать через СМИ, что врагов нет, при этом обсуждать отдельные исторические периоды и интересы отдельных народностей (цель: общество как целое должно исчезнуть в качестве объекта сознания); 2) заставить общество слушать только противника, не обращая внимания на какие-то иные мысли или ощущения, например, акцентировать средства массовой информации исключительно на какой-то одной парадигме общественного развития, например западной, исключив любой другой опыт: Китай, Японию, мусульманский мир (цель: процесс нагружения общественного сознания и действие формирующих сил ослабляются); 3) заставить общество не размышлять над тем, что говорит противник, для этого исключить из СМИ серьезные аналитические исследования проблем (цель: способствовать торможению непрерывного потока мыслей); 4) сосредоточить внимание общества на каком-то предмете помимо входного информационного потока, например, внутренние катаклизмы, войны, акты террора (цель: подсистема защиты, ответственная за обработку входной информации, оказывается не в состоянии выполнять свою функцию и как бы расстраивается); 5) постоянно внушать, что само общество становится лучше и лучше, что все окружающие относятся к нему лучше и лучше (цель: подобное внушение ослабляет историческую память и чувство самоотождествленности, которыми характеризуется нормальное состояние общества); 6) СМИ одновременно должны убеждать членов общества, что возникшее состояние— это не совсем то, что должно быть (цель: создание пассивного состояния сознания, в котором сохраняется возможность зависимости от информационного воздействия противника).

Приведенный алгоритм в общих чертах отражает работу СМИ в России времен 1990—1997 гг.

Для точной и своевременной обработки входной информации элементы любой ИС должны "питаться", а связи между ними поддерживаться в работоспособном состоянии. Отсюда естественным образом следует, что эффективность целенаправленного ИВ резко увеличивается, если оно сочетается с другими видами воздействия на информационную самообучающуюся систему.

Что же собой представляют эти «другие виды воздействия»? Любая система, ответственная за обработку входных данных, должна «питаться», т.е. должна потреблять энергию для того, чтобы приводить в действие заложенные в ней алгоритмы обработки входных данных и генерировать новые. Базовые элементы каждой системы имеют определенную физическую природу, которая во многом определяет время реакции, а значит, и выбор того или иного алгоритма решения конкретной задачи.

Понятно, что если речь идет о такой информационной самообучающейся системе, как человек, то системы питания йога, созерцающего собственный пуп в условиях вечного лета, и жителя крайнего севера должны быть различны. И эти различия должны касаться не только количества энергии, заключенного в потребляемой пище, но и ее микроэлементного состава. Системы «Йог» и «Эскимос» обрабатывают разные входные данные, требующие от подсистемы принятия решения в большинстве своем различных выходных результатов. Сказанное косвенно означает, что для того, чтобы возможности Йога по перепрограммированию Эскимоса на эталон, которым является собственное подобие, возросли, того надо кормить той же самой пищей.

Интересное и оригинальное исследование воздействия пищи и различных наркотических приправ на возможность превращения обезьяны в человека и на поведение современного человечества приведено в работе Теренса Маккенна «Пища богов». Он, в частности, считает, что уровень развития и достижения современных цивилизаций во многом определился и определяется практикой их питания.

В случае рассмотрения в качестве информационных самообучающихся систем государств под «другими видами воздействия» в свете вышесказанного следует понимать в первую очередь экономическую войну. Но не в узком плане, связанном исключительно с экономическими санкциями типа

«это нельзя и это нельзя», а в более широком, включающем в себя «экономические интервенции» в виде товаров и продуктов по демпинговым ценам.

Время информационных и экономических войн пришло еще и потому, что сегодняшнему миру уже не свойственен дефицит информации и промышленных товаров, наоборот, его отличает именно их избыток. А это значит, что, как и в случае информационной войны, когда система больше должна думать не о защите информации, а о защите от информации и продвижении своего видения мира, так и в условиях экономической войны, речь должна идти о защите от чужих товаров и навязывании своих.

Грамотное сочетание всех допустимых видов воздействия на противника представляет собой комплексную стратегию воздействия. Под допустимыми видами воздействия здесь понимаются такие воздействия, которые «грубо» не нарушают принятые в обществе на текущее время нормы и правила поведения. Следование принципу комплексности при формировании общей стратегии воздействия на противника позволяет усилить эффект от применения информационного оружия и тем самым может являться еще одним признаком информационной войны.

3. Последствия информационной войны

Прежде чем перейти к исследованию последствий информационной войны, желательно ответить на один принципиальный вопрос: существуют ли признаки, на основании которых можно судить о степени поражения системы в информационной войне? Если исходить из того, что информационная война ничем от обычной войны, кроме применяемого оружия, не отличается, то и признаки поражения должны быть точно такими же.

А чем характеризуется система, потерпевшая поражение в обычной войне? Пусть эта система— обычное государство. Тогда для потерпевшей поражение страны в той или иной степени характерно, как показывает практика первой и второй мировых войн: 1) гибель и эмиграция части населения; 2) разрушение промышленности и выплата контрибуции; 3) потеря части территории; 4) политическая зависимость от победителя; 5) уничтожение (резкое сокращение) армии или запрет на собственную армию; 6) вывоз из страны наиболее перспективных и наукоемких технологий.

Обобщение сказанного для информационных самообучающихся систем может означать: 1) стабильное сокращение информационной емкости системы, гибель элементов; подобное упрощение системы делает ее безопасной для агрессора; 2) решение ранее несвойственных задач, т.е. задач в интересах победителя. Потенция ИС направлена на отработку входных данных победи-

теля; 3) побежденная система как бы встраивается в общий алгоритм функционирования победителя, т.е. поглощается структурой победителя.

Таким образом, особой разницы для потерпевшей поражение системы от того, в какой войне: ядерной или информационной, она проиграла, нет. Разница может быть только в том, что информационная война не имеет финала, так как проблема окончания информационной войны, как и проблема ее начала, относится к алгоритмически неразрешимым проблемам. Более того, нет причин, по которым агрессор прекратил бы свое воздействие на жертву.

После всего сказанного осталось рассмотреть возможные результаты информационной войны, о которых не думает развязавшая ее сторона.

Так, в случае войны огнестрельным автоматическим оружием победителю достаются разрушенные города, уничтоженные и покалеченные человеческие ресурсы. И это понятно: огнестрельное оружие в первую очередь направлено на уничтожение военной техники и живой силы противника.

Ядерным оружием бьют уже по мирному населению, и, как показал опыт его применения США к японским городам, - на равнинах оно более эффективно. До сегодняшнего дня оно применялось в основном для того, чтобы продемонстрировать свою силу, а потом диктовать запуганной жертве правила поведения. Нежелательные же последствия ядерной войны - ядерная зима.

Информационная оружие направлено непосредственно на изменение поведения ИС, а в случае применения против людей — на изменение их мышления и соответственно поведения без предварительного «запугивания».

Таким образом, прослеживается определенная иерархия в типах войн, охватывающих человечество, и применяемом в этих войнах оружие, направленном на (этапы): - уничтожение; - запугивание; - изменение поведения.

В конце-то концов цель любой войны заключается в изменении поведения противника, в постановке его на то место, где его хотелось бы видеть. Но если все предыдущие войны вели к желаемому результату через запугивание и уничтожение, то при информационной войне это делается непосредственно напрямую и может продолжаться сколь угодно долго, до тех пор, пока «кот сам не захочет отпустить мышь».

Так каковы же могут быть дополнительные последствия информационной войны, кроме желаемых, кроме таких, когда «в ответ в вас летят мешки с долларами, фунтами, марками и франками?

Победителем информационной войны становится та сторона, которая более полно способна промоделировать поведение противника в различных ситуациях, определить собственный алгоритм поведения и реализовать его.

Более полно промоделировать поведение противника — это значит в больших объемах собирать, хранить и обрабатывать информацию о противнике: это значит более полно изучить поведение противника — знать и понимать его историю, культуру, религию, быт и т.п.

Для решения этой задачи наилучшими инструментами являются средства вычислительной техники (СВТ) с соответствующим ПО. Ситуационное моделирование в режиме реального времени сегодня вполне по плечу высокопроизводительным комплексам; проблема только в реализуемой поведенческой модели конкретных социальных объектов, конкретных людей. И проблема эта тем лучше решается, чем больше информации об анализируемых и моделируемых объектах.

Понятно, что результаты от применения компьютерных моделей тем качественнее, чем серьезнее используемая платформа, включающая в себя: вычислительные мощности, интеллектуальные возможности программистов-математиков, опыт специалистов, работающих в области практической поведенческой психологии. Серьезность платформы, к сожалению, определяется не идеалами, а финансами. Поэтому, у кого основные капиталы у того более совершенное информационное оружие. В отличие от химического или ядерного, да даже просто, огнестрельного оружия на применение ЭВМ (основного элемента информационного оружия) нет законодательного запрета ни в одной стране мира. Говорильни же о запрете информационного оружия выглядят просто смешными, так как запрет этот ни теоретически, ни практически невозможно проконтролировать. Компьютеры доступны всем. Вопрос только в том, кто первый выстрелит и сумеет «дожать» ситуацию.

Безусловно, информационные войны на нашей планете велись с тех пор, как люди научились говорить, понимать и соответственно этому пониманию запугивать друг друга. Но эффективность подобных информационных операций по сравнению с применением даже примитивного холодного оружия «оставляла желать лучшего». Это объяснимо. Стрела из лука долетит быстрее и сделает больше, чем долгое и нудное объяснение словами, которое к тому же обязано быть убедительным, а иначе оно не способно дать рост мыслям именно в нужном направлении. Компьютер и средства глобальной телекоммуникации изменили окружающее пространство. Теперь воздействовать информацией стало проще, быстрее, безнаказанней, а самое главное, дешевле, чем любым другим видом оружия. Отдельные информационные ручейки между людьми и странами благодаря средствам вычислительной техники и телекоммуникационным системам слились в одну сплошную реку,

которую уже невозможно запрудить, ее даже невозможно перекрыть «рыболовными сетями».

Время на передачу сообщений свелось к нулю. Время на осмысление полученной информации благодаря соответствующим технологиям также резко сократилось. В этой ситуации что-то делать для информационной защиты традиционными пассивными методами стало бессмысленно.

Более того, используя современные высокопроизводительные компьютеры, появляется возможность создавать искусственные миры и выдавать их за реальные. И как говорится: СВТ сегодня вполне позволяют в режиме реального времени создать виртуальную модель объекта и его связей, а затем проецировать ее на окружающий мир, на зрителей, ожидающих события.

За всем сказанным не только стоит возможность корректировки и подмены выступлений политических лидеров, приказов командующих боевыми соединениями, но проступают черты и более глобальных мистификаций.

Таким образом, любое государство может эффективно себя защищать в сфере информационного противодействия исключительно активными методами, т.е. применением всех средств ИВ, включая компьютерное моделирование, по всему спектру внешних и внутренних врагов. Именно прогнозное компьютерное моделирование является той сетью, которая набрасывается на мир информационных систем, заставляя эти системы постоянно наращивать собственные мощности, порождая контроль, контроль за контролем и т.д.

Исходными данными систем, функционирующих в социальном пространстве, являются общегосударственные и частные базы данных на граждан, предприятия, услуги, товары и т.п.

Объемы этих баз постоянно растут. Туда заносится не только фамилия, имя и отчество, туда заносится весь жизненный путь, включая состояние здоровья на этом пути. А зная прошлое иногда проще прогнозировать будущее.

В описанных выше условиях побежденному в информационной войне не остается никаких шансов на ответный удар. И он это осознает. Поверженный в информационной войне интуитивно понимает, что любое его логически обоснованное рациональное поведение уже просчитано и запрограммировано врагом. Единственное, что ему остается, — это иррациональное поведение.

Результатом информационной войны становится иррациональное поведение поверженных систем, это их единственный путь «встать на ноги». Иррациональное поведение это хаос, это бесцельная смута, это терроризм.

При этом наибольший эффект террористические акции могут дать их организаторам через террористическое воздействие на объекты кибернетического пространства. «Самой заманчивой целью для терроризма нового поколения следует признать деловые центры обработки информации, прежде всего компьютеризованные банковские учреждения.

Террористический удар СВЧ-излучения по крупному банку способен вызвать системный кризис финансовой системы развитых стран, поскольку он лишает общество доверия к современным технологиям денежного рынка».

Однако, сделав столь категорический вывод, они, возможно, забыли учесть одно маленькое обстоятельство, заключающееся в том, что про факт террористического воздействия на крупный банк общество скорее всего ничего не узнает, так как, когда выгодно владельцам СМИ, они могут дружно навесить ярлык отрицания на любую, даже самую сенсационную информацию. Но, кроме того, всегда надо помнить, что сегодня СМИ уже являются классическим информационным оружием, принадлежащим тому, кто платит, т.е. правящей верхушке, и применяются для управления собственным народом в собственных интересах.

Контрольные вопросы

1. Пояснить на примере зависимость устойчивости системы к целенаправленному информационному воздействию от мощности базовых элементов.
2. Дать характеристику алгоритма информационной войны.
3. Применение «Протоколов собраний Сионских мудрецов».
4. Проблемы защиты от информации и продвижение своего видения мира.
5. Чем характеризуется система, проигравшая в информационной войне?
6. Охарактеризовать победителя и побеждённого в информационной войне.
7. Роль ситуационного моделирования для ведения информационной войны.
8. СМИ как классическое информационное оружие.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. -392с.
2. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.
3. Стратегия национальной безопасности Российской Федерации (Указ Президента РФ от 31.01.2015 г. № 683).
4. Доктрина ИБ информационной безопасности РФ от 05.12.2016 (Указ Президента РФ от 05 декабря 2016 г.).
5. Стратегия национальной безопасности Российской Федерации: Утв. Указом Президента РФ от 31 декабря 2015г. № 683.
6. Малюк А.А. Защита информации в информационном обществе. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2015. – 230 с.
5. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 с.

1.