ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

191-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовым работам по дисциплине
«Социотехнические основы
информационной безопасности»
для студентов специальностей
090301 «Компьютерная безопасность»,
090302 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составители: д-р техн. наук А. Г. Остапенко, ассистент М. В. Бурса

УДК 004.415.2

Методические указания к курсовым работам по дисциплине «Социотехнические основы информационной безопасности» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. А. Г. Остапенко, М. В. Бурса. Воронеж, 2015. 68 с.

Методические указания посвящены вопросам проектирования социотехнических систем в условиях реализации информационных операций и атак. В ходе выполнения курсовой работы студенты должны приобрести необходимые практические навыки по основным методам анализа риска в динамике угроз, закрепить знания, полученные в лекционном курсе.

Методические указания подготовлены в электронном виде в текстовом редакторе и содержатся в файле Остапенко_КР_СоцТех_основы_ИБ.pdf.

Табл. 6. Ил. 14. Библиогр.: 88 назв.

Рецензент д-р техн. наук, проф. О.Н. Чопоров

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А.Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

Информационные операции и атаки наиболее часто рассматриваются в контексте описания возникающих в современных социотехнических системах конфликтов и противоборств с применением информационного оружия, приобретая то или иное содержание в зависимости от модели нового социального и технического устройства общества. Сейчас информационное противоборство становится приоритетной формой борьбы за виртуальное право использовать политические, экономические, дипломатические, военные и другие способы для воздействия на информационную среду конкурента и защиты в интересах достижения собственных эгоцентрических целей. Причем военная сфера уже давно стала лишь частью площадки ведения своеобразных информационных игр на этом поприще, где поиск истины в последней инстанции имеет большую сложность по причине отсутствия эффективных международных и национальных юридических норм.

Защита осложняется наличием: нарастающей радиоэлектронной борьбы, технической разведки, информационного терроризма, посягательств на различные виды тайн, особенно в экономическом и хозяйственном управлении, возрастающей ликвидностью правонарушений в области связи и информации, пограничной латентностью компьютерных преступлений с повышением уровня их общественной опасности.

Вместе с тем: в праве появилось новое соотношение ключевых понятий знака и реальности, в уголовном законе утвердился запрет на совершение преступлений в сфере компьютерной информации, в административно-правовых нормах – соответствующие санкции за нарушение порядка в области регулирования связи и доступа к информации и др. Операционные безналичные деньги и бездокументарные ценные бумаги утратили «телесные» носители. Объекты недвижимости, записи актов гражданского состояния, юридические лица и индивидуальные предприниматели получили идентификацию в данных. Гражданские правоотношения сместились в вирту-

альное пространство с особыми методами взаимодействия субъектов по фактам электронной цифровой подписи, совершения сделок в сети Интернет, защиты охраняемых законом тайн и т.п.

Увы, по объективным причинам позитивное право не всегда обеспечивает адекватное правовое регулирование новых общественных отношений и находится только на подступах к созданию стройной концепции информации как объекта прав и объекта преступных посягательств. Задача выделения информационных операций и атак из всех возможных шаблонов действий в области соответственно частного и публичного права на сегодняшний день остается во многом нерешенной.

Отсюда рельефно выступает проблема поведения в ходе реализации информационных операций и атак. Она обусловлена избыточностью в эмпирических материалах, казуальных схемах, концептуальных и доктринальных нормах декларативной бланкетной направленности и дедуктивными недостатками в материальном и виртуальном мире, инфраструктуре, общих моделях, универсальном регулировании.

Таким образом, становится очевидной необходимость формирования комплексных интегративных подходов к рассмотрению информационных операций и атак как стадий информационных конфликтов и противоборств социотехнических систем.

1. СОЦИОТЕХНИЧЕСКИЕ СИСТЕМЫ КАК СРЕДА РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ И АТАК

1.1. Анализ подходов к определению понятия «социотехническая система»

На сегодняшний день сложилось несколько подходов к применению понятия социотехнических систем (СТС). Они обусловлены спецификой определенных областей научных знаний: 1) менеджмента; 2) информациологии; 3) социального управления. Д. Грейсон, К. О' Делл предполагают органическое сочетание развития технической и социальной подсистем управления трудовыми процессами, предлагая две модели СТС (рис. 1, 2).

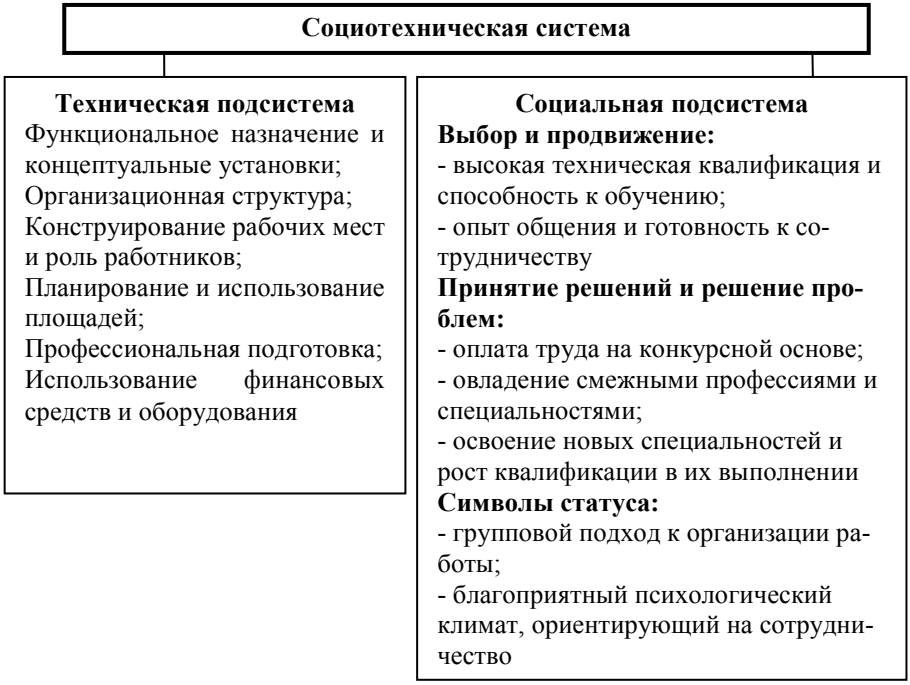

Рис. 1. Простая модель социотехнической системы

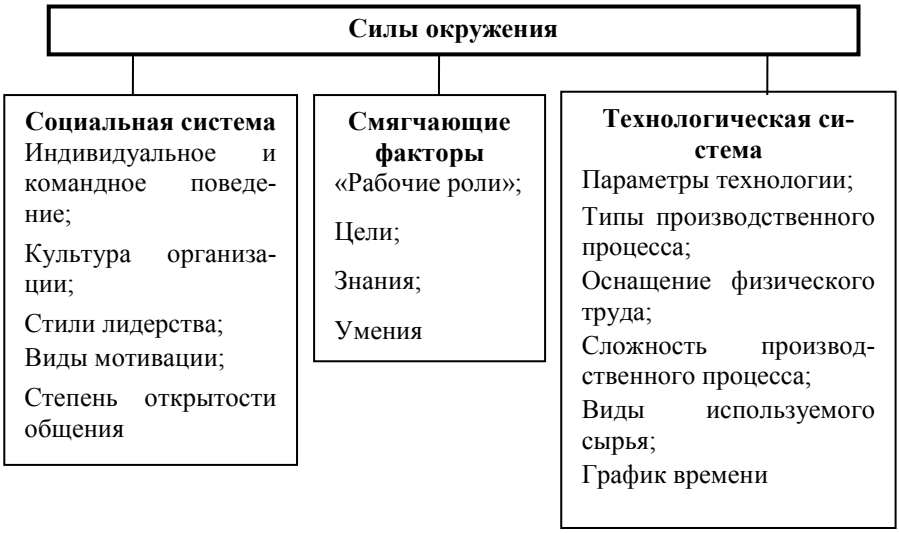

Рис. 2. Сложная модель социотехнической системы

Простая и сложная модели СТС строятся на принципах, определяемых факторами инновационности, развитием человеческих ресурсов, гибкости связи с окружающей средой, кооперации, ответственности и производительности, создания общих оптимальных условий.

С.В. Волобуев рассматривает СТС как современные объекты информатизации с угрозами в отдельных подсистемах, источниками излучений информативных сигналов, каналами утечки сообщений, через которые последние распространяются, каналами информационного воздействия.

Данные авторы, моделируя информационные операции и атаки в сфере государственного и муниципального управления, отождествляют СТС с региональным информационным пространством (ИП) и включают в СТС региона совокупность автоматизированных информационно-коммуникационных систем, технологий, а также сообщество взаимодействующих с ними людей.

ИП формируется силами окружения (рис. 2), довлеющими над составляющими ИП социальной и технической под-

систем, включая обостряющие и смягчающие факторы, законы функционирования СТС.

Явившаяся комплексной проблема безопасности ИП в условиях информационных операций и атак (ИОА) суммарно охватывает обозначенные области, поэтому целесообразно синтезировать относительно универсальную модель, позволившую выявить закономерности функционирования и подстерегающие опасности социотехнических информационных систем в информационно-психологическом и информационно-кибернетическом пространстве (ИПП и ИКП).

Обобщенный вариант модели СТС применительно к ИП изображен на рис. 3.

При этом СТС в ИП как правило имеет ярко выраженную триаду

$$S(R, K, \Gamma),$$

где R – множество ресурсов (в данном случае информационных);

K – множество коммуникаций;

Γ – предикат (закон), определяющий технические и социальные регламенты функционирования СТС.

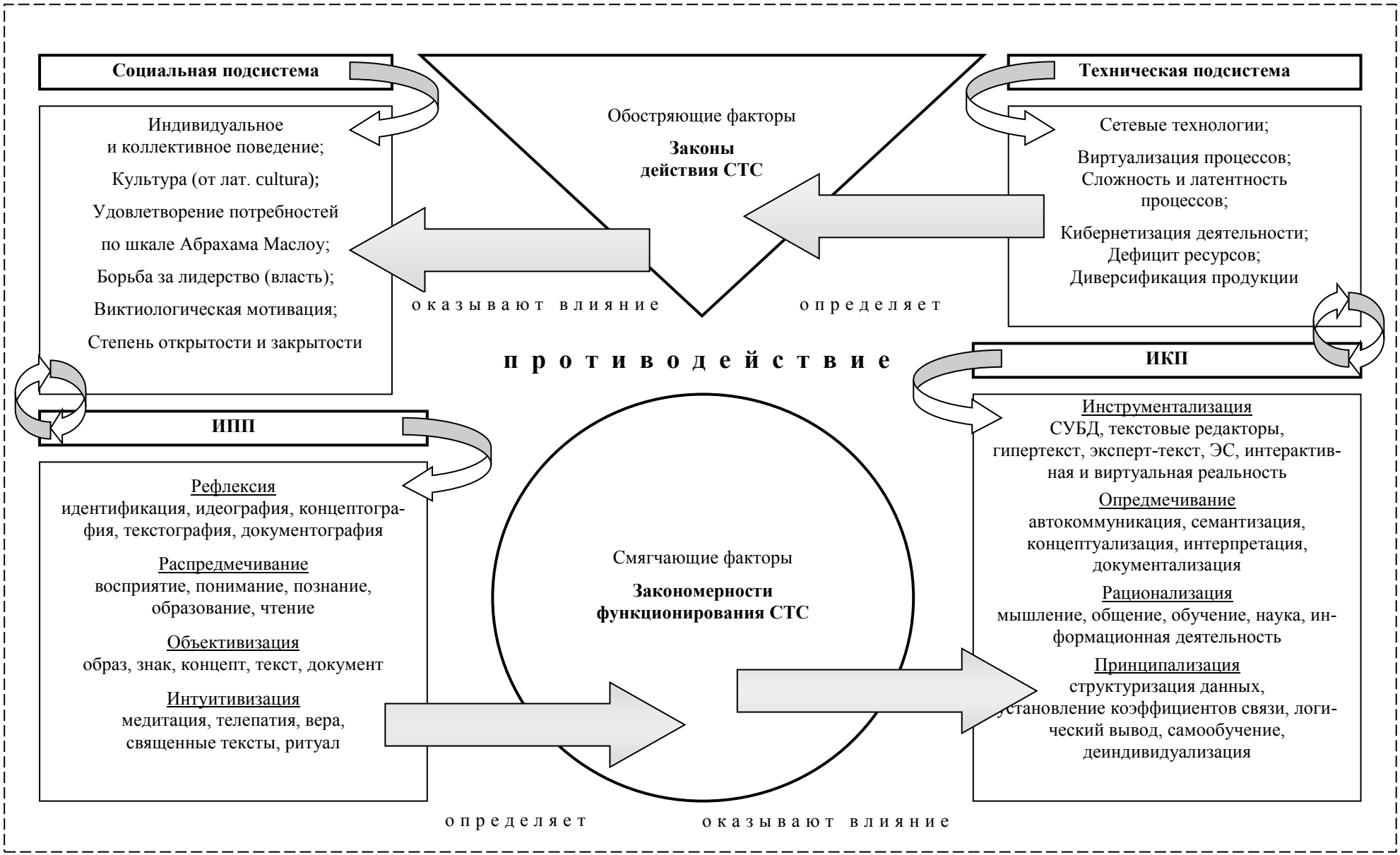

Рис. 3. Обобщенный вариант модели социотехнической системы

В техническом аспекте Γ задает индиденцию элементов R и K, условия информационного взаимодействия субъектов S в ИП, включая облик баз и банков данных, каналов связи, центров обработки информации и управления.

Сравнительная кибернетизация современного общества, очевидно, требует рассмотрения всех вышеперечисленных атрибутов ИП в аспекте обеспечения безопасности ИКП. Совокупность научно-технических поисков и результатов в данном направлении представляет собой вполне самостоятельную область человеческих знаний, включающую:

- техническую теорию информации;
- техническую и криптографическую ЗИ;
- аппаратные и программные средства;
- программирование оборудования и ПО;
- проектирование и внедрение автоматизированных, сетевых, телекоммуникационных систем;
- новейшие молекулярные теории гарантий дальнейшей кибернетизации.

Однако для СТС не представляется возможной только кибернетическая регламентация. Социальная компонента и человеческий фактор обуславливают необходимость применения права, и предикат Γ обязательно имеет организационно-правовую составляющую $\Gamma^{(ОП)} \subset \Gamma$.

Ее можно раскрыть по следующим позициям:

- организация и правовой режим защиты информации согласно базовым федеральным законам, руководящим документам ФСТЭК России, государственным стандартам;
- «собственничество» в информации открытого доступа систем общего пользования;
- «шифрование» в информации закрытого доступа систем пользования ограниченного круга лиц;
- защита исключительных (патентных прав) на оборудование систем;

- организация связи, электронной торговли, ведение государственных и иных реестров;
- привлечение к ответственности за нарушения закона в ИП.

Систематизировать обозначенные позиции можно по признакам состояния регулирования в национальной правовой системе (табл. 1).

Правоприменительная практика в данном случае, прежде всего, направлена на снижение неоднозначности информационных отношений, т.е. в какой-то степени на минимизацию энтропии СТС. Регламентация и регулирование жизни общества в информационной сфере с каждым днем приобретает все более существенное значение.

Отсюда важнейшей составляющей предиката Γ очевидно выступает организационно-правовая компонента, регламентирующая информационные отношения субъектов ИП (рис. 4).

Предикат Γ также имеет организационно-правовую компоненту деструктивных отношений в ИП (рис. 5).

Таблица 1

Позиции предиката по признакам состояния правового регулирования

Позиции	Урегулировано	Нуждается в совершенствовании регулирования	Не урегулировано
1	**2**	**3**	**4**
Организация и правовой режим защиты информации	Конституционные информационно-правовые нормы; информационно-правовые нормы Гражданского Кодекса РФ; ФЗ «Об информации, информационных технологиях и защите информации»; Руководящие документы ФСТЭК РФ; государственные стандарты в области ТЗИ	Земельный Кодекс РФ, Бюджетный Кодекс РФ, Лесной Кодекс РФ, Воздушный Кодекс РФ, Водный Кодекс РФ, Градостроительный Кодекс РФ. Настоящие кодексы необходимо дополнить нормами по обеспечению сохранности информации в электронных записях ФОИВ	Процессуальные диспозитивные нормы перечисленных актов в области технической защиты информации общего пользования, деструктивное использование которой способно причинить вред СТС ключевых инфраструктур, не содержащих информацию, составляющую гостайну – НГК, ЖД, АВС и пр.
«Собственничество» в информации открытого доступа систем общего пользования	Конституционные информационно-правовые нормы; ФЗ «О библиотечном деле», «О средствах массовой информации», «О рекламе»	Закон РФ «О средствах массовой информации»	Комплексное право на информацию – законопроекты «О праве на информацию», «Об информационной открытости» и пр.

Продолжение табл. 1

1	2	3	4
Защита исключительных (патентных) прав на оборудование систем	Законы РФ «Об авторском праве и смежных правах», «О правовой охране программ для электронных вычислительных машин и баз данных», «О правовой охране топологий интегральных микросхем», Патентный Закон до 1 января 2008 г. С 1 января –IV часть ГК РФ	Материальные и процессуальные нормы актов об исключительных правах в их кумулятивном значении	Институт обязательственного права в области регулирования лицензионных соглашений
«Шифрование» в информации закрытого доступа систем пользования ограниченного круга лиц	Гражданско-правовые нормы о тайнах (банковской, служебной, страховой, личной, семейной); Налоговый Кодекс РФ; Трудовой Кодекс РФ; Основы законодательства РФ об охране здоровья граждан; Закон РФ «О государственной тайне», ФЗ «О персональных данных», «О коммерческой тайне», «Об аудиторской деятельности», «Об адвокатской деятельности и адвокатуре»; Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера»; стандарты организации (Банка России и пр.)	Гражданско-правовые нормы о страховой тайне; ФЗ «О коммерческой тайне»	Конструкция служебной тайны - законопроект «О служебной тайне»

Окончание табл. 1

1	2	3	4
Организация связи, электронной торговли, ведение государственных и иных реестров	Конституционно-правовые нормы; ФЗ «О связи», «Об электронной цифровой подписи», «О техническом регулировании», «О рынке ценных бумаг», «О несостоятельности» (банкротстве), «О государственной регистрации юридических лиц и индивидуальных предпринимателей», «О государственном земельном кадастре», «О государственной регистрации прав на недвижимое имущество и сделок с ним»	ФЗ «О связи» применительно к коммуникации в сети Интернет	Подотрасль электронной торговли в информационном праве – законопроект «Об электронной торговле»; правовой режим электронного документооборота, как в государственных, некоммерческих, так и коммерческих организациях – законопроект «Об электронном документообороте»
Привлечение к ответственности за нарушения закона в ИП	Кодекс Российской Федерации об административных правонарушениях, Уголовный Кодекс РФ, Гражданский Кодекс РФ, Трудовой Кодекс РФ, Уголовно-процессуальный Кодекс РФ, Гражданский процессуальный Кодекс РФ	Уголовный Кодекс РФ необходимо дополнить составами за мошенничество с применением информационных технологий	Юридическая ответственность за деструктивное информационно-психологическое воздействие (гипноз, психологические приемы и эффекты в процессе проведения ИОА)

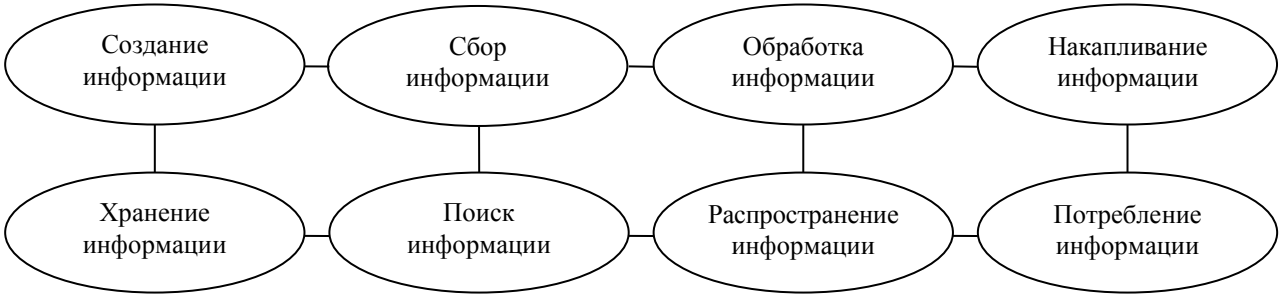

Рис. 4. Организационно-правовая компонента предиката, регламентирующая информационные отношения субъектов ИП

Рис. 5. Организационно-правовая компонента предиката для деструктивных отношений

Таблица 2

Правовые (легальные) и неправовые определения деструктивных компонент предиката

Деструктивные отношения	**Правовые (легальные) определения**	**Неправовые определения**
1	**2**	**3**
Утечка	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Убывание информации по электрическим, электромагнитным, параметрическим (акустическим и пр.) каналам; Неконтролируемый выход информации за пределы круга лиц, которым эта информация доверена
Искажение	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Предоставление заведомо ложных или неполных данных и/или сведений, вводящих заинтересованных лиц в заблуждение
Задержка	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Опаздывание и промедление в обслуживании вызова и доставки данных
Блокирование	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Обеспечение недоступности данных и/или сведений и/или сообщений, невозможности их использования в результате искусственного затруднения доступа пользователей к какому-либо устройству, системе или сети ЭВМ при сохранении самой информации

Продолжение табл. 2

1	2	3
Утрата	Лица, виновные в умышленном или неосторожном искажении либо утрате информации о правах на недвижимое имущество и сделках с ним, зарегистрированных в установленном порядке, несут ответственность за материальный ущерб, нанесенный в связи с этим какой-либо из сторон, в соответствии с законодательством РФ – ФЗ «О государственной регистрации прав на недвижимое имущество и сделок с ним» № 122-ФЗ от 21 июля 1997г.	Выход данных и/или сведений из владения определенного лица помимо его воли
Потеря	Трансляция в прямом эфире или в записи спортивного соревнования, в котором не предусмотрены перерывы или остановки, может прерываться рекламой таким образом, чтобы прерывание трансляции не привело к потере части существенной информации о спортивном соревновании – ФЗ «О рекламе» № 38-ФЗ от 13 марта 2006г.	Возникновение убытка и/или упущенной выгоды и/или проигрыша, ущерба, убыли, лишения
Переадресация	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Услуга сетей с коммутацией пакетов, обеспечивающая направление вызова по другому сетевому адресу в том случае, если не работает канал, соединяющий коммутатор с устройством, имеющим первоначальный адрес. В телекоммуникационных системах - операция инициирования сеанса связи

Продолжение табл. 2

1	2	3
Уничтожение	Лотерея, проводимая в режиме реального времени, если договор об участии в лотерее заключается сторонами путем обмена документами посредством электронной или иной связи с использованием лотерейного оборудования, которое объединено сетью электросвязи, позволяет достоверно установить, что документ исходит от стороны договора, и с помощью которого проводятся розыгрыш призового фонда лотереи в режиме реального времени, фиксация и передача информации о результатах такого розыгрыша. Указанное оборудование должно обеспечивать защиту такой информации от утраты, хищения, искажения, подделки, а также от несанкционированных действий по ее уничтожению, модификации, копированию и иных подобных действий и несанкционированного доступа к сети электросвязи – ФЗ «О лотереях» № 138-ФЗ от 11 ноября 2003г.	Приведение данных и/или сведений и/или сообщений в полную негодность, когда они навсегда утрачивают свою предметную ценность и не могут быть использованы по своему назначению
Перехват	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Перехват сообщений ПЭМИ, акустических сигналов или путем ВЧ-облучения ТСОИ

Окончание табл. 2

1	2	3
Подделка	Основное технологическое оборудование и оборудование для учета объема оборота и (или) использования для собственных нужд этилового спирта, алкогольной и спиртосодержащей продукции должны быть оснащены техническими средствами фиксации и передачи информации об объеме производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции в единую государственную автоматизированную информационную систему, включающими в себя средства защиты информации, предотвращающие искажение и подделку фиксируемой и передаваемой информации – ФЗ «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции» № 171-ФЗ от 22 ноября 1995г.	Полное или частичное изготовление данных и/или сведений и/или сообщений неуполномоченным лицом
Дублирование	ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России	Исполнение данных в системе банков и баз данных в двух экземплярах, их сдваивание, выполнение сходных (одинаковых) действий, направленных на достижение определенной цели, мотивированной корыстными либо низменными побуждениями

Рассматривая (рис. 6) конфликты подсистем ИП с законом субъектов ИП Γ, можно утверждать для S_1 и S_2 их законы Γ_1 и Γ_2 индуцированы Γ, который к сожалению допускает проведение ИОА и деструктивные отношения (рис. 5) в ИП.

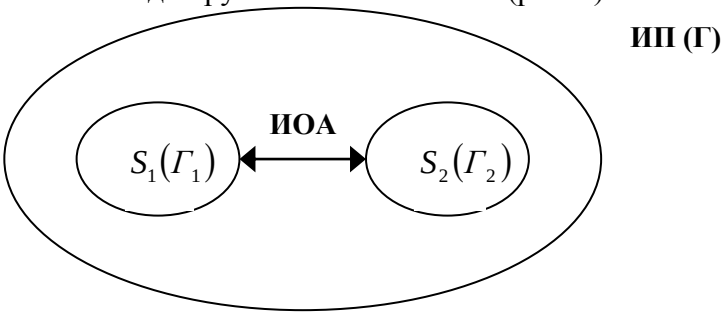

Рис. 6. Схема деструктивных отношений в ИП

Деструктивные отношения в ИП обычно провоцируются информационными конфликтами (рис. 6), обусловленными противоречивостью целей взаимодействующих подсистем $W_1(S_1)$ и $W_2(S_2)$.

Проблема гармонизации Γ, Γ_1 и Γ_2, снижающей риск успеха деструктивных ИОА и обеспечивающей траекторию устойчивого развития, как в отношении всего ИП, так и для его отдельных субъектов (S_1 и S_2), фактически является предметом исследования настоящей работы.

В этой связи рассмотрим, прежде всего, общие закономерности существования СТС в контексте вероятной реализации ИОА.

1.2. Общие закономерности функционирования социотехнических информационных систем

Закономерности функционирования СТС по большому счету выступают смягчающими факторами, так как нивелируют возникновение случайных неуправляемых процессов; позволяют с определенной достоверностью решать поставленные стратеги-

ческие и тактические задачи, являются ограничительными и предупреждают о том, какие состояния и тенденции в развитии заведомо следует избегать, и тем самым оказывают позитивное управляющее влияние на информационную деятельность. Учет системных закономерностей позволяет спрогнозировать и в требуемой степени детерминировать информационные процессы, возникающие в конфликтных, кризисных (квазибифуркационных) ситуациях и определить наиболее эффективные пути выхода из них и/или способы противодействия ИОА.

Причем закономерности функционирования СТС носят относительно универсальный характер и пригодны в отношении как ИПП, так и ИКП. Смягчающими факторами во время проведения ИОА можно считать «рабочие роли» компонентов, участников (объектов и субъектов) в зависимости от целей, стратегии, миссии системы, когда преднамеренно дозируются отдельные элементы составляющих социальной и технической подсистем СТС в сторону ослабления, смягчения, редукции, ущерба от реализации ИОА. В задании предполагается оценки эффективности обеспечения информационной безопасности вышеуказанных объектов.

1.2.1. Энтропийная компенсация, динамическое равновесие или баланс

СТС описываются в терминах энтропии и антиэнтропии при негэнтропии, т.е. меры беспорядка (хаоса) и порядка, неопределенности и определенности, неорганизованности и организованности. Обеспечение энтропийного равновесия между порядком и беспорядком определяет индивидуальное и коллективное поведение СТС в ИПП и ИКП, различного уровня информационные процессы, условия их возникновения, изменения и развития.

Характеристики социальной и технической подсистем СТС как носителей положительной, отрицательной и нулевой энтропии в условиях реализации ИОА приведен в табл. 3.

Важно отметить, что негэнтропия или связанная информация, существуют во всех элементах СТС. Связанная информация детерминируется первичными, производными информационными потоками и обладает способностью существенно понижать энтропию в ходе проведения ИОА.

Таблица 3

Характеристики упорядоченности социальной и технической подсистем

Вид энтропии (положительная, нулевая и отрицательная)	Вид упорядоченности	Характеристики упорядоченности социальной и технической подсистем СТС в условиях реализации ИОА	
Положительная энтропия или просто энтропия ($Э$)	Неопределенность, беспорядок или хаос частичный или полный, неорганизованность	социальной Индивидуальное и коллективное поведение с нарушенной психикой, иногда с нормальной психикой; виктиологическая мотивация; рефлексия в сознании; интуитивизация в сознании	технической Виртуализация процессов, их сложность и латентность; инструментализация в сознании
Нулевая энтропия ($Э = 0$)	Полный порядок, полная определенность, отсутствие хаоса, организованность	Культура; удовлетворение потребностей по шкале Абрахама Маслоу; борьба за лидерство (власть); объективизация в сознании	Сетевые технологии; кибернетизация деятельности; дефицит ресурсов; диверсификация продукции; рационализация и принципализация в сознании

Продолжение табл. 3

Вид энтропии (положительная,нулевая и отрицательная)	Вид упорядоченности	Характеристики упорядоченности социальной и технической подсистем СТС в условиях реализации ИОА	
		социальной	технической
Антиэнтропия или отрицательная энтропия $(-Э)$	Самоорганизация, полная самоуправляемость, саморазвитие	Степень открытости и закрытости; распредмечивание в сознании	Опредмечивание в сознании

В ИП может встретиться изолированная или закрытая СТС S_3, состоящая из двух закрытых, или изолированных (не контактирующих) систем S_1 и S_2, имеющих множество допустимых состояний, где $|A_1|$ – число допустимых состояний системы S_1, а $|A_2|$ – системы S_2. Тогда $Э_3 = \ln(|A_3|) = \ln|A_1| + \ln|A_2| = Э_1 + Э_2$.

Возникают случаи, когда закрытое или изолированное ИП S не взаимодействует с инородными СТС, но в свою очередь состоит из двух открытых или взаимодействующих (в рамках S) систем S_1 и S_2 (рис. 6). Для такой СТС действует закономерность энтропийной компенсации, которая заключается в том, что понижение $Э_1$ в одной подсистеме S_1, и следовательно, увеличение порядка, требует обязательного повышения $Э_2$, и следовательно, увеличение беспорядка в другой подсистеме S_2, чтобы они компенсировали друг друга, ибо $Э_1 + Э_2 = Э = const$. Получается, если две или больше, открытые СТС взаимодействуют друг с другом, и вместе составляют изолированную (закрытую) СТС, тогда общая закрытая система S остается **равновесной, если изменение энтропии одной системы будет равно измене-**

нию энтропии другой системы с противоположным знаком. Исходя из указанной закономерности энтропийной компенсации, следует, что, доминирующая система, реализуя ИОА, снижает свою энтропию (а, следовательно, улучшают свое состояние) за счет повышения энтропии других систем, завоевывая ИП, осуществляя информационную экспансию и сбрасывая избытки энтропии в эти системы.

Успехи одних СТС возможны в глобальном ИП только при одновременных неуспехах и неудачах других СТС. Поэтому, **всеобщее благоденствие СТС в ИП несбыточно, а конфликты неизбежны.** Поэтому для оптимизации параметров ИП используется **закономерность энтропийного динамического равновесия** или баланса.

Эта закономерность **определяет состояние динамического равновесия между порядком и беспорядком**, между организованностью и дезорганизованностью различных СТС и в значительной степени предопределяет причины конфликтов, возникновения замысла и реализации ИОА. В точке, где обе противодействующие компенсируют друг друга, возникает энтропийное равновесие ($Э_р$) или критический уровень организации $Э_к$. Точка энтропийного равновесия между порядком и беспорядком СТС показана на рис. 7.

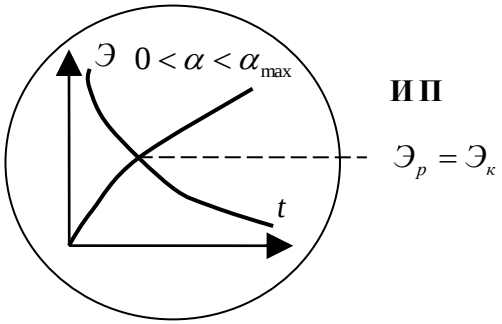

Рис. 7. Энтропийное динамическое равновесие или баланс

Так как в точке энтропийного равновесия ($Э_р$) или на критическом уровне организации ($Э_к$), процессы деорганизации и упорядочивания ИП уравновешивают друг друга – в СТС возникает стабильность. Удержание стабильности всегда критично, что ведет к выбору альтернативы из трех способов управления энтропийными процессами в СТС. **Первый способ** основан на смещении линий энтропийного равновесия $Э_р(Э_{р1}, Э_{р2}, Э_{р3}) = Э_к$ путем изменения степени открытости СТС $(\alpha_1, \alpha_2, \alpha_3)$ за счет изменения внешнего воздействия сил окружения (F_1, F_2, F_3) ИПП и ИКП (рис. 8).

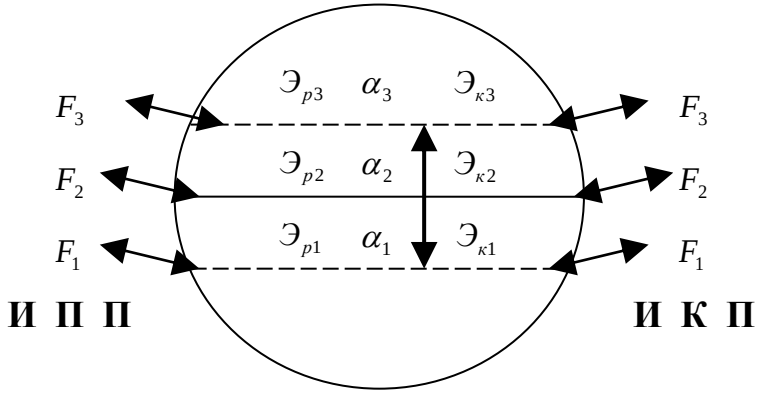

Рис. 8. Первый способ управления энтропийными процессами в социотехнических системах

В процессе изменения энтропии в СТС из-за инерционности возникают энтропийные колебания относительно энтропийного равновесия или критического уровня ($Э_р = Э_к$), которые могут затухать со временем, и СТС становится стабильной. Рост амплитуды и частоты энтропийных колебаний приводит к усилению негативных явлений: растет вероятность появления стихийности их организации и проведения, разрушения используемых ресурсов, увеличивается острота и частота виктиологической мотивации, латентности информационных процессов (рис. 9).

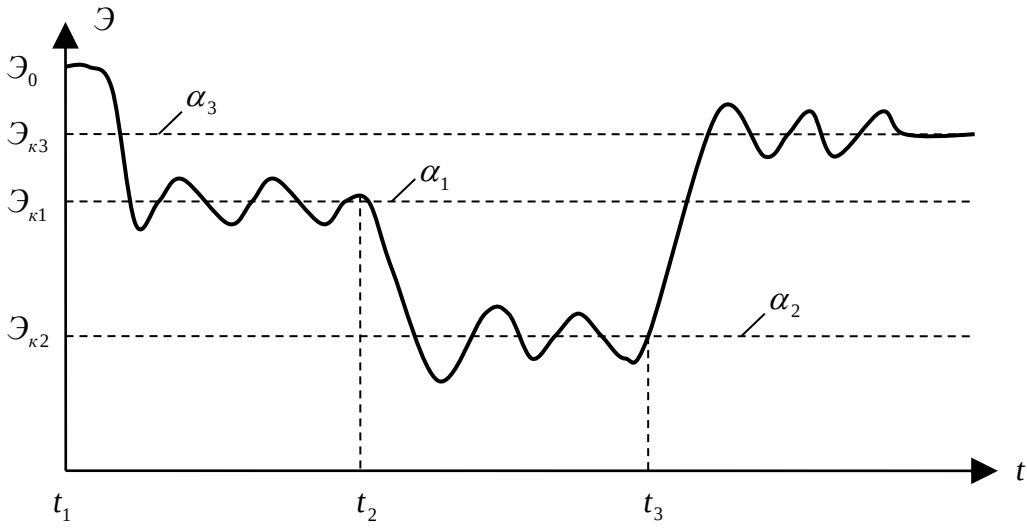

Рис. 9. Энтропийные колебания относительно энтропийного равновесия

Примером установления энтропийного равновесия, несмотря на амплитудные и частотные колебания, служит сложившийся в ИП порядок (рис. 10) в отношении информационных ресурсов открытого и закрытого доступа (сведений конфиденциального характера, государственной тайны).

На рис. 9 критический уровень организации $(Э_0, Э_{к1}, Э_{к2}, Э_{к3})$ при изменении степени открытости СТС $(\alpha_1, \alpha_2, \alpha_3)$ приобретает значения, соответствующие разным степеням открытости СТС. Увеличение степени открытости в момент t_2 приводит к организации до нового критического уровня $Э_{к2}$, а ее уменьшение в момент времени t_3 – к дезорганизации до нового критического уровня $Э_{к3}$.

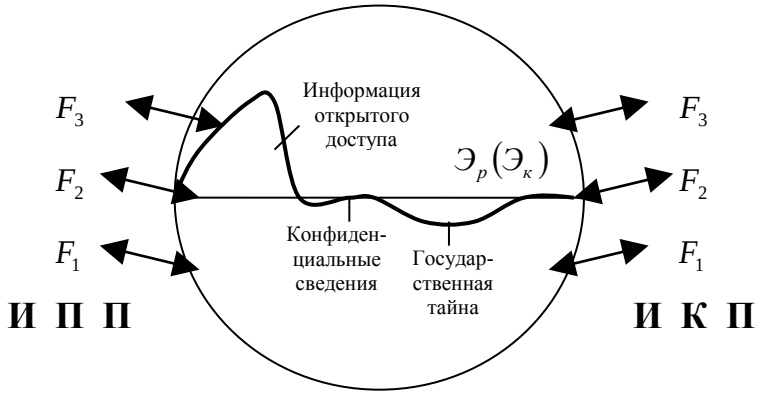

Рис. 10. Пример установления энтропийного равновесия в отношении информации открытого и закрытого доступа

Таким образом, **второй способ** управления энтропийными процессами в СТС заключается в управлении амплитудой и частотой энтропийных колебаний, чтобы их снижать и, следовательно, иметь ущерб от ИОА реже и меньший по величине (рис. 11).

Третий способ управления упрощенно показан на рис. 12. Здесь для обеспечения большего порядка и большей организованности необходимо вынести из собственной СТС излишнюю энтропию в другие СТС ИПП и ИКП.

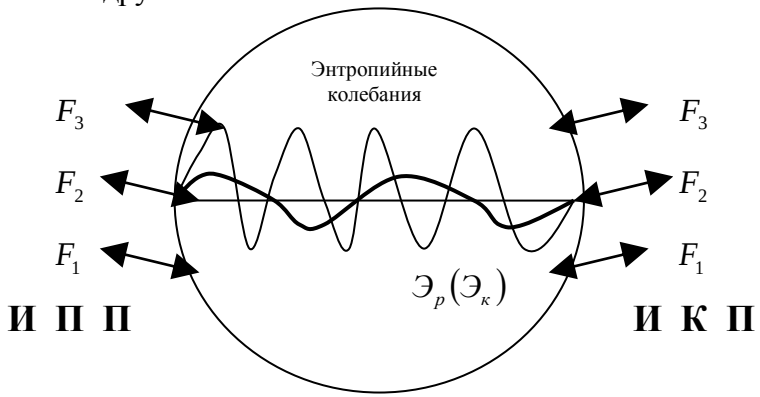

Рис. 11. Второй способ управления энтропийными процессами в социотехнических системах

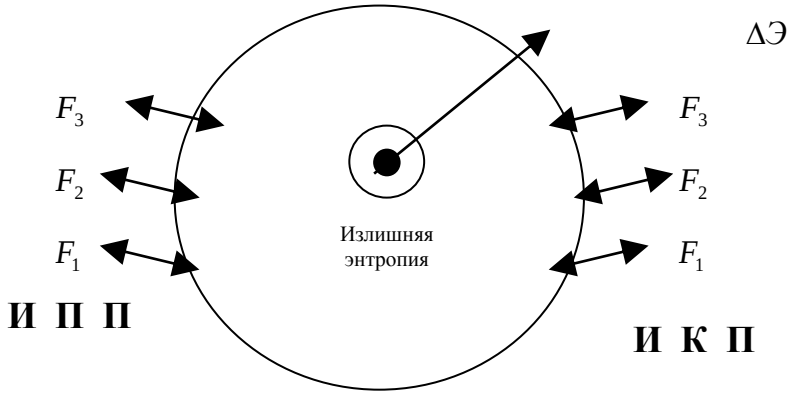

Рис. 12. Третий способ управления энтропийными процессами в социотехнических системах

Как правило, излишняя энтропия по закону упорядочения Γ выносится из отдельных элементов составляющих СТС, являющихся носителями положительной энтропии: общественное осуждение информационного пиратства и борьба с компьютерными правонарушениями; принудительная ликвидация деструктивных сект; реализация контртеррористических операций по предупреждению и ликвидации последствий терактов в ИП, включая кибертерроризм и т.п.

1.2.2. Колебательные и циклические принципы функционирования

Следующей важной закономерностью, во многом определяющей сценарии ИОА в ИПП и ИКП, являются колебательные и циклические принципы функционирования СТС, которые непрерывно переходят из одного состояния в другое и обратно. Из глобальной истории развития СТС явствует два антагонистических процесса: 1) индивидуализация и концентрация в руках групп лиц, создающих и поддерживающих ИПП и ИКП ограниченного круга; 2) институализация во всеобщих ИПП и ИКП. Изучая малую локальную историю СТС, обнаружим срез глобальных процессов, их дробление в зависимости от целей, стра-

тегии, миссии конкретной СТС. В настоящее время СТС, входящие в тот или иной процесс, постепенно вступают во все более тесные отношения, все чаще комбинируя или вовсе смешивая их. Открываясь, СТС получают практически неограниченные возможности для проведения ИОА (роста риска).

Цикличность СТС означает, что определенные процессы и явления развития СТС повторяются через определенные периоды времени. Изучение колебаний цикличности позволит изучить сущность повторяемости кризисов, конфликтов, подъемов и спадов. Например, получаемый в период успеха излишек ресурсов накапливается в СТС для последующего использования в периоды спадов и кризисов, а накопление резерва ресурсов при подъеме позволяет сгладить последствия колебаний в цикле.

1.2.3. Зависимость потенциала системы от структуры и от характера взаимодействия ее структурных элементов

Потенциал СТС является основой ее эффективной деятельности, поэтому повышение потенциала СТС представляет задачу первостепенной важности.

Под потенциалом СТС будем понимать жизненно важные ресурсы составляющих социальной и технической подсистем СТС, включая отдельные элементы сознания, которые могут быть приведены в действие для того, чтобы достичь определенной цели. Жизненно важные ресурсы могут определяться как количественными, так и качественными характеристиками. Например, качество технологий; количество видов используемых информационных ресурсов, открытых и закрытых систем; параметры коммуникационных возможностей; качество элементов рефлексии и разветвленность информационной инфраструктуры. Указанные ресурсы назовем относительными, так как реализация ИОА может их изменить, перераспределить, перепрограммировать и т.п.

Метафизические ресурсы ИП и времени, включая ИПП и ИКП, представляются абсолютными, не подлежащими корректированию в результате ИОА. В ходе развития систем абсолютные

ресурсы актуализируются всегда. Относительные ресурсы напротив актуализируются, как правило, частично, маневрируя понижением или повышением потенциала. Так, например, чем выше ресурсоемкость информационно-коммуникационных технологий (ИКТ), тем выше степень открытости СТС.

Управление (посредством Γ) потенциалом СТС и его оптимальное использование обеспечивается благодаря возможности концентрации ресурсов на отдельных компонентах R и K в краткосрочные сроки, долгосрочные сроки в периоды различных колебаний в цикле.

Потенциал СТС зависит от того, насколько целенаправленно, взаимосогласованно и рационально взаимодействуют элементы между собой и насколько рационально организована сама система, ее составляющие. Чем выше целенаправленность и взаимосогласованность действий элементов СТС, тем выше ее организованность и меньше энтропия.

При эмерджентности (Γ) потенциал СТС многократно превышает сумму потенциалов всех элементов составляющих социальной и технической подсистем СТС: $P(S) > \sum_i P(S_t)$. Что касается энтропии СТС, то она меньше, чем сумма энтропии входящих элементов из-за четкого и согласованного взаимодействия элементов системы. Если при интеграции (объединении) энтропия системы уменьшается, это означает, что имеет место новое интегративное свойство СТС $Э(S) < \sum_i Э(S_t)$.

Интеграция может оказать неэффективной, т.е. степень организованности СТС не обеспечила эффективного и согласованного взаимодействия элементов составляющих социальной и технической подсистем СТС, потенциал СТС равен сумме потенциалов составных элементов: $P(S) = \sum_i P(S_t)$.

Энтропия такой СТС равна сумме энтропии составных элементов. Следовательно, здесь имеет место не эмерджментность, а суперпозиция.

Развитие сопровождается множеством ошибок и кризисов, так или иначе приводивших к спадам и поражениям, которые выявляют неорганизованность СТС, когда взаимодействие элементов составляющих социальной и технической подсистем СТС носит

неуправляемый или случайный (хаотический) характер.

Потенциал СТС равен потенциалу ее отдельного усредненного элемента: $P(S) = [P(S_1) + P(S_2) + ...P(S_n)]/n$ или $P(S) = [P(S_1), P(S_2), ..., P(S_n)]$.

В случае возникновения антагонистических противоречий и эскалации конфликтов в среде СТС, когда каждый элемент составляющих социальной и технической систем СТС противодействует всем остальным («война каждого со всеми»), потенциал СТС меньше потенциала самого слабого элемента системы, а энтропия системы, наоборот, больше энтропии самого слабого элемента системы $P(S) < \min_i [P(S_i)]$, $Э(S) > \min_i [Э(S_i)]$.

1.3. Законы существования социотехнических систем, объясняющие дуализм существования информационно-психологического и информационно-кибернетического пространства

Закономерности СТС, выражающие их универсальный характер, не объясняют дуализм существования ИПП и ИКП.

Хотя очевидно, что действие СТС не происходит самопроизвольно даже с учетом закономерностей их функционирования, для этого нужен специальный «агрегат», который бы всякий раз приводил к реализации механизм развития. Таким «агрегатом» действия СТС выступают законы $Г$, по своей природе являющиеся принуждающими элементами в системе и обостряющие отношения в системе. В отличие от юридических законов они представляют собой более системные, общеобязательные, объективные, связанные с технологиями правила, не имеющие волевого характера, но в конечном итоге определяемые алгоритмами составляющих социальной и технической подсистем СТС.

Законы призваны внедрять в СТС регуляцию средств организации и ресурсов, блокируя деструктивные формы процессов и явлений в механизме ИОА и стимулируя конструктивность. В результате подобной регуляции формируется ИП, фиксирую-

щее в велениях законов СТС ориентиры для организации деятельности, закрепляющее процессы и явления развития.

Схоластическое расположение ИПП и ИКП в социокультурном пространстве исходит от признания равноправными двух начал: социального, тесно связанного с психологией, и технологического, причинно-обусловленного кибернетикой. Несмотря на сложность поссибилизма и пробабализма здесь не наблюдается противостояние дуализма плюрализму, так как ИПП и ИКП, обуславливая неминуемый взаимообмен в СТС, зависят от одних и тех же смягчающих и обостряющих факторов, восполняют пробелы и дополняют друг друга при противодействии ИОА.

Поэтому ИПП и ИКП не только отличаются дуализмом существования, но и субсидиарным (акцессорным) порядком собственных взаимоотношений. Причем не принципиально, какое из пространств в конкретном механизме ИОА играет ведомую роль. Примером может служить Холодная война СССР и США, где ИОА проводились как в ИПП в процессах поддержки диссидентского движения, вещания радио «Голос Америки», явления маккартизма и пр., так и в ИКП в «гонке вооружений», космических исследованиях, создании компьютерных сетей и т.д. В годы после Второй мировой войны ведомую роль играло ИПП в явлении доктрины сдерживания социализма Трумэна, а, начиная с 60-х г.г. – ИКП в процессе Карибского кризиса и достижении военного паритета СССР с США. С учетом дуализма представляется целесообразным определить ИПП и ИКП следующим образом.

Информационно-психологическое пространство – схоластически расположенное в информационном пространстве, равное в отношении информационно-кибернетического пространства, тесно связанное с психологией, фиксирующее в велениях законов СТС ориентиры для организации деятельности (включая ИОА) и одновременно являющееся фоном, закрепленных информационно-кибернетическим пространством процессов и явлений.

Информационно-кибернетическое пространство – схоластически расположенное в информационном пространстве, рав-

ное в отношении информационно-психологического пространства, причинно-обусловленное кибернетикой, фиксирующее в велениях законов СТС ориентиры для организации деятельности (включая ИОА) и одновременно являющееся фоном, закрепленных информационно-психологическим пространством процессов и явлений.

Вышеизложенное схематично изображено на рис. 13.

1.3.1. Организация, ограничение, опережение, неполное использование, искажение, принудительное отчуждение и обобществление информации

Первым законом является закон организации и ограничения информации в СТС. Чем выше уровень организованности СТС, тем выше уровень ограничений на использование информации из различных видов ресурсов, особенно в ходе противодействия ИОА.

Действительно, степень закрытости СТС в части государственной тайны ограничивается большими барьерами в сравнении со степенью закрытости СТС в части тайны коммерческой. Соответственно подсистемы, использующие ресурсы государственной тайны, существеннее ограничены в информационных потоках по сравнению с подсистемами, применяющими корпоративные схемы.

Для СТС известен закон информационного опережения, который означает, что решение проблем развития СТС должно опережать по времени каждый очередной шаг в отдельных элементах составляющих социальной и технической подсистем СТС, что дает возможность точнее координировать отдельные процессы и явления, создавать благоприятные условия для функционирования механизма развития, обеспечивать равноправие на актуализацию фона со стороны ИПП и ИКП. В конечном счете запаздывание информационных потоков приводит к дезорганизованности целевых СТС.

Рис. 13. Законы действия социотехнических систем, объясняющие дуализм существования информационно-психологического и информационно-кибернетического пространства

В области информационной деятельности СТС действует правило неполного использования информации, в том числе при принятии решений управленческого характера, что определяется как парадоксом избыточности информации, так и неспособностью элементов интеллекта (сознания) предпринять необходимые меры к принципализации информационного потенциала (см. рис. 3).

В ходе распространения информации действует закон искажения информации по мере движения, что связано, как с техническими, организационно-правовыми проблемами защиты информации, так и с различной способностью и готовностью элементов сознания к ее восприятию.

В результате потребления информационной дозы, вброшенной в СТС, действует правило принудительного отчуждения и обобществления информации.

В более организованных СТС принудительное отчуждение спрограммировано составляющими технической подсистемы СТС по командам подсистемы социальной. Обобществления информации, а именно ее нейтрального принятия без оценки опасности и использования в определенных интересах здесь зачастую не происходит.

В менее организованных СТС принудительное отчуждение производится отдельными элементами составляющих социальной и технической подсистем совокупным, почти хаотическим способом, по принципам «чем больше, тем лучше», «чем меньше, тем лучше» и пр. Здесь наблюдается частичное или полное обобществление информации.

1.4. Опасности социотехнических систем

Основываясь на теории безопасности, представляется целесообразным употребить термин «опасности» СТС вместо «угрозы» СТС в связи с формированием в России нового порядка технического регулирования. Опасность – возможность чего-нибудь нежелательного, является понятием большим по объему по сравнению с понятием угрозы и дает возможность совместить последнее с риском, как в организационном, так и правовом ас-

пектах.

Угроза в уголовном праве – выраженное словесно, письменно, действиями либо другим способом намерение нанести физический, материальный или иной вред лицу или общественным интересам; один из видов психического насилия над личностью.

Угроза совершить опасное преступление (например, угроза убийством, нанесением тяжких телесных повреждений или уничтожением имущества путем поджога) по российскому праву влечет уголовную ответственность и рассматривается как самостоятельное оконченное преступление.

Угроза в международном праве – противоречащие принципу запрещения применения силы и угрозы силой действия, создающие вопреки Уставу ООН угрозу территориальной неприкосновенности или политической независимости какого-либо государства, а также совершенные каким-либо др. образом, не совместимым с целями ООН.

В отличие от применения силы, констатируемого при помощи Определения агрессии 1974 г., до настоящего времени отсутствуют какие-либо международные документы, конкретизирующие понятие «У.п.с.».

На основе имеющейся практики можно различать насильственные действия психологического и материального характера, обладающие значением У.п.с. О психологической У.п.с. можно говорить применительно к действиям государства, выражающиеся в пропаганде войны. Материальная У.п.с. проявляется в таких действиях, как концентрация на границе вооруженных сил и вооружений в размерах, превышающих обычно размещаемые, морские демонстрации вблизи берегов др. государства, размещение оружия в пространствах, обычно не используемых в военных целях (космическое пространство, дно морей и океанов и т.д.).

В качестве У.п.с. могут рассматриваться не вызываемые потребностями самообороны действия государства по наращиванию своего военного потенциала. Право констатации У.п.с. в действиях какого-либо государства принадлежит тому государству, безопасность которого ставится в результате этих действий под угрозу.

Такого рода действия могут быть оценены Советом Безопасности ООН в качестве угрозы миру и вызвать с его стороны осуществление коллективных мер, предусмотренных гл. VII Устава ООН. Что касается реакции на У.п.с. со стороны непосредственно пострадавшего от нее государства, то она может приобрести форму ответных действий идентичного характера – самозащиты.

Из изложенного следует, что дискурсивным является применение понятия угрозы, выраженного уголовным правом, как обобщающего в опасностях СТС, а угрозы применения силы, обозначенного международным правом – ограничительного в опасностях государственных (национальных), межгосударственных (межнациональных) СТС.

Риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда позволяет учесть не только качественную, но и количественную сторону опасностей СТС, причем как видно из определения в организационном и правовом аспектах.

Механизм оценки опасностей и рисков в СТС схематически представлен на рис. 14.

1.4.1. Опасности в информационно-психологическом пространстве

Опасности в ИПП – это возможности отрицательных, негативных, нежелательных проявлений в схоластически расположенном информационном пространстве, тесно связанном с психологией личности, групп и масс, в том числе в результате реализации ИОА.

Как правило, возможности отрицательных, негативных, нежелательных проявлений в ИПП прямо зависят от возможностей положительных, желательных проявлений в ИПП, и последние обуславливают возникновение и действие первых (табл. 4), т.е. имеет место некий дуализм.

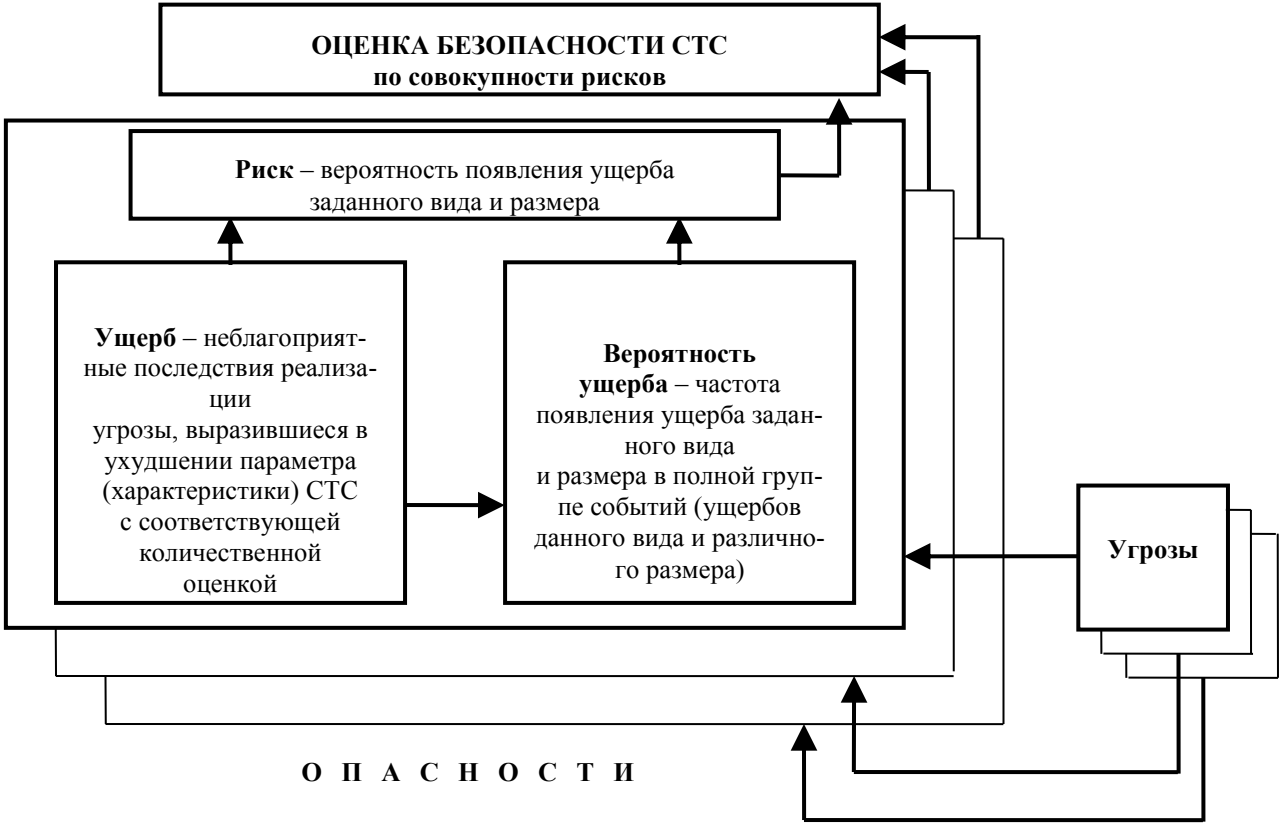

Рис. 14. Механизм оценки опасностей и рисков в социотехнических системах

Таблица 4

Опасности в информационно-психологическом пространстве

Положительные, желательные проявления в ИПП	**Возможности отрицательных, негативных, нежелательных проявлений в ИПП**
Культура и общество	
Свободное развитие индивида	Автоматизация жизнедеятельности человека
Информационное общество	Дегуманизация жизни
Социализация информации	Технократическое мышление
Коммуникативное общество	Снижение культурного уровня
Преодоление кризиса цивилизации	Лавина информации. Элитарное знание (поляризация)
Социальное партнерство	Изоляция индивида
Информационно-кибернетическая безопасность	Компьютерная преступность
Информационно-психологическая безопасность	Усиление социальных кризисов после информационных резонансов
Политика	
Расширение демократии	Ограничение свобод
Децентрализация управления	Централизация власти
Выравнивание иерархии власти	Государство-«надзиратель»
Расширенное участие в общественной жизни	Засилие государственной бюрократии
Укрепление дружбы народов	Усиление виктиологической мотивации благодаря информационным потокам и вбросам
Правовое государство	Усиление манипуляции людьми
Хозяйство и труд	
Повышение продуктивности. Рационализация труда	Все возрастающая сложность и теснота жизни
Повышение компетентности. Увеличение богатства на основе здоровой конкуренции	Обострение промышленного шпионажа

Продолжение табл. 4

Положительные, желательные проявления в ИПП	**Возможности отрицательных, негативных, нежелательных проявлений в ИПП**
Преодоление кризиса информационно-экономической диспропорции	Концентрация информации в руках экономической элиты
Экономия потенциала и ресурсов	Подверженность кризисам в актуализации двадцати процентов ресурсов
Охрана окружающей среды	Экологическая безопасность
Децентрализация промышленности. Новая продукция	Массовая безработица. Новые требования к мобильности трудящихся
Улучшение качества труда	Дегуманизация труда
Диверсификация продукции	Проблема утилизации. Контрафактная продукция
Новые профессии и квалификации	Деквалификация. Исчезновение многочисленных профессий с ядром
Социальная справедливость	Диспропорция доходов
Рациональное природопользование	Бедствия, аварии, катастрофы, исчерпание ресурсов
Международные отношения	
Национальная независимость	Усиление зависимости от супердержав
Шанс на устойчивое развитие у стран «третьего мира»	Технологическая зависимость. Обострение отношений развитых и развивающихся стран
Улучшение обороноспособности государств и международной безопасности	Уязвимость. Обострение информационных конфликтов. Появление статики информационных противоборств и динамики информационного оружия

Угроза применения силы в ИПП со стороны государственных (национальных), межгосударственных (межнациональных) СТС может быть совершена только путем использования возможностей отрицательных, негативных, нежелатель-

ных проявлений ИПП (например, угроза диверсией, бедствием, аварией, катастрофой, исчерпанием ресурсов, террористической акцией, межнациональным конфликтом).

Угрозы в ИПП со стороны любых СТС выражаются словесно, письменно, в результате ИОА либо другим способом с намерением нанести материальный (физический, имущественный), моральный, организационный, интеллектуальный вред ИПП СТС. Угрозу в данном случае СТС вправе воспринять как один из видов психического насилия. Например, угроза компьютерным преступлением, промышленным шпионажем, террористическая угроза и т.п.

Риски в ИПП показывают вероятности причинения вреда отдельным элементам составляющих социальной подсистемы СТС в двух состояниях:

1) состояние, при котором присутствует недопустимый риск – опасное состояние ИПП, т.е. в составляющих элементах социальной подсистемы не обеспечивается безопасность от реализации ИОА;

2) состояние, при котором отсутствует недопустимый риск – безопасное состояние ИПП, т.е. в составляющих элементах социальной подсистемы обеспечивается защищенность от воздействия организационного механизма ИОА с определенной эффективностью.

Достижение недопустимого риска и его дальнейшее нивелирование объясняется закономерностями функционирования и законами действия СТС.

1.4.2. Опасности в информационно-кибернетическом пространстве

Опасности в ИКП – это возможности отрицательных, негативных, нежелательных проявлений в схоластически расположенном информационном пространстве, обусловленному законами кибернетики, в том числе в результате реализации ИОА.

Так же, как и в ИПП, возможности отрицательных, негативных, нежелательных проявлений в ИКП дуальны, т.е. они, как

правило, прямо зависят от возможностей положительных, желательных проявлений в ИКП, и последние ведут к возникновению и действию первых (табл. 5).

Таблица 5

Опасности в информационно-кибернетическом пространстве

Положительные, желательные проявления в ИКП	**Возможности отрицательных, негативных, нежелательных проявлений в ИКП**
Технологии	
Компьютерные сети	НСД, вирусы и пр.
Виртуальный мир Интернет	Взломы сайтов, хищение информации с серверов, мошенничество в сфере электронной коммерции, кредитных карточек и пр.
Программные комплексы ERP планирования ресурсов организации	Нарушение работы электронной финансовой системы и бухгалтерского учета в организации
Программные комплексы SCADA технологическими процессами	Срыв электронного контроля и сбора первичных данных
Программные комплексы MES управления производственными процессами	Электронное покушение на сроки эксплуатации оборудования, учет энергетических затрат, контроль качества готовой продукции, резервирование деталей
Электронные СМИ	Появление информационного оружия. Информационные операции и атаки
Информационно-справочные системы	Ограничение открытого доступа к информации
----------	----------
Управление	
Информационно-телекоммуникационные системы государственного управления	Несвоевременное принятие управленческих решений, сокрытие информационных фактов, отказ в предоставлении информации и пр.

Продолжение табл. 5

Положительные, желательные проявления в ИКП	**Возможности отрицательных, негативных, нежелательных проявлений в ИКП**
Информационно-телекоммуникационные системы муниципального управления	Несвоевременное принятие решений местного значения, сокрытие реальной обстановки в социальной сфере, социальная напряженность и пр.
Информационно-телекоммуникационные системы корпоративного управления	Смена организационно-правовой формы, недобросовестная конкуренция, реорганизация и ликвидация юридических лиц, появление монополий, дочерних и зависимых обществ и пр.
----------	----------
Ресурсы	
Информационные ресурсы закрытого или ограниченного доступа (государственная тайна и другие виды тайн)	Государственная измена, крайняя финансовая неустойчивость корпораций, незаконное использование интеллектуальной собственности, покушение профессиональное соответствие и моральный облик специалистов-профессионалов, причинение ущерба путем разглашения тайны усыновления, нотариальной и пр. тайн
Информационные ресурсы открытого доступа (сети общего пользования)	Нарушение работы управляющих и аналитических центров
Государственные реестры (регистры)	Несвоевременность записей и недостоверность предоставляемой информации

Угроза применения силы в ИКП со стороны государственных (национальных), межгосударственных (межнациональных) СТС может быть совершена только путем использования возможностей отрицательных, негативных, нежелатель-

ных проявлений ИКП (например, угроза государственной изменой, применением информационного оружия и пр.).

Угрозы в ИКП со стороны любых СТС выражаются словесно, письменно, действиями ИОА либо другим способом с намерением нанести материальный (физический, имущественный), моральный, организационный, интеллектуальный вред ИКП СТС. Угрозу в данном случае СТС вправе воспринять как один из видов психического насилия. Например, угроза НСД, нарушением электронной системы контроля качества готовой продукции, распространением сведений, порочащих деловую репутацию, возникновением социальной напряженности и т.п.

Риски в ИКП показывают вероятности причинения вреда отдельным элементам составляющих технической подсистемы СТС в двух состояниях:

1) состояние, при котором присутствует недопустимый риск (по вероятности и масштабам ущерба) – опасное состояние ИКП, в составляющих элементах технической подсистемы СТС не обеспечивается безопасность от воздействия организационного механизма ИОА;

2) состояние, при котором отсутствует недопустимый риск (по вероятности и масштабам ущерба) – безопасное состояние ИКП, в составляющих элементах технической подсистемы СТС обеспечивается защищенность от реализации ИОА с определенной эффективностью.

В ИКП также, как и в ИПП достижение недопустимого риска и его дальнейшее нивелирование объясняется закономерностями функционирования и законами действия СТС, механизмами реализации ИОА и противодействия им.

Следует отметить, что сегодня опасности в ИПП и ИКП имеют неоднозначное правовое проецирование, т.е. они чаще всего не поддаются надлежащей правовой оценке с позиции действующих правовых норм в системе права.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Цель и задачи курсовой работы

Курсовая работа (КР) является важной составной частью самостоятельной работы студента. Целью курсовой работы является закрепление и углубление знаний в области обеспечения информационной безопасности социотехнических систем (СТО-ИБ).

Написание КР позволяет научиться работать с информационными источниками, анализировать и систематизировать их делать соответствующие выводы.

Кроме того, это ещё и формы контроля уровня профессиональной подготовки обучающихся, и потому данные работы выполняются с соблюдением единых требований и правил ГОСТ и СТП 62-2007.

КР должна быть творческой, самостоятельной работой, показывающей способность студента разбираться в теоретических и практических вопросах, уметь систематизировать материал по выбранной теме, связно изложить и творчески использовать теоретические идеи и положения. При этом проект не должен носить компилятивный характер, и тем более, не быть плагиатом: недопустимы как прямое заимствование без точного указания источников, так и простой пересказ и изложение учебной и методической литературы. Цитаты, мысли других авторов, факты и даже идеи, пересказанные своими словами, должны в обязательном порядке иметь однозначные указания, ссылки на источник (в том числе и соответствующие адреса в Интернете).

Выполнение КР является заключительным этапом обучения студентов по дисциплине «Социотехнические основы информационной безопасности», аттестацией, позволяющей оценить уровень их подготовленности по соответствующему направлению, способности к самостоятельному решению проектных, психологических, экономических, организационно-управленческих и других задач.

Задачи, которые должен выполнить студент, для реализации поставленной цели:

– анализ и исследование угроз СТОИБ;

– систематизация, закрепление и расширение теоретических знаний и практических навыков в области обеспечения СТОИБ;

– построение математических моделей процессов реализации информационно-психологических угроз в отношении;

– построение моделей коммуникаций в контексте обеспечения СТОИБ;

– развитие навыков ведения самостоятельной работы и овладения методикой исследования и экспериментирования при решении разрабатываемых проблем и вопросов.

В ходе выполнения курсовой работы студенту необходимо решить следующие задачи:

– постановка цели и задач КР;

– обзор информационных источников по тематике КР;

– анализ выбранных информационных источник;

– описание основных положений курсовой работы;

– исследование и анализ угроз СТОИБ (построение математической модели процессов реализации угроз и построение модели коммуникаций в контексте обеспечения СТОИБ);

– систематизация полученных результатов;

– формулирование выводов по работе.

2.2. Содержание и объём курсовой работы

Основные требования к КР установлены стандартом предприятия СТП ВГТУ 62-2007. КР состоит из расчетно-пояснительной записки (РПЗ) объёмом от 30 до 50 страниц печатного текста с иллюстративным графическим материалом, размещенным по разделам работы, чертежей, схем.

РПЗ содержит следующие разделы:

а) титульный лист является первой страницей РПЗ;

б) задание на курсовую работу;

в) лист «Замечания руководителя»;

г) реферат, аннотация (при необходимости);

д) содержание включает введение, наименование всех разделов, подразделов, пунктов (если они имеют наименование), заключение, список литературы, наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки;

е) введение;

ж) основную часть (расчетную, исследовательскую) содержащую: литературный обзор, анализ задания на КР, выбор и обоснование метода исследования проблемы, исследование по выбранному методу выбранной проблемы;

з) заключение;

и) список литературы;

к) приложения (при необходимости).

Пояснительная записка может быть дополнена и другими разделами.

2.3. Этапы выполнения курсовой работы

1. Выбор темы. Тема КР выбирается студентом самостоятельно (из перечня, предложенного преподавателем), но окончательно тема согласовывается с преподавателем. Выбор темы КР необходимо соотносить с изучаемым как теоретическим, так и практическим курсом, т.к. именно наличие систематических знаний и изучение специальной терминологии позволит студенту понять тему, а изучив соответствующую литературу, раскрыть тему, сделав теоретические и практические выводы, а также рекомендации по теме обзора, используя знания и умения, полученные при обучении (1 неделя со дня выдачи преподавателем списка тем КР).

2. Изучение англоязычных источников по теме. Допускается автоматизированный перевод с последующим редактированием текста (2-3 недели со дня выбора темы КР).

3. Составление библиографии: подбор студентом литературы по выбранной теме КР (3 недели со дня выбора темы КР).

4. Конспектирование необходимого материала или составление тезисов.

5. Систематизация зафиксированной и отобранной информации.

6. Определение основных понятий темы и анализируемых проблем.

7. Разработка логики исследования проблемы, составление плана (перечня основных положений, которые предстоит раскрыть).

8. Реализация плана, написание КР (3-4 недели).

9. Самоанализ, предполагающий оценку новизны, степени раскрытия сущности проблемы, обоснованности выбора источников и оценку объема КР.

10. Проверка оформления списка литературы.

11. Редакторская правка текста.

12. Оформление КР и проверка текста с точки зрения грамотности и стилистики.

13. Сдача КР на проверку преподавателю (до зачётной недели).

3. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ И ОБЪЕМУ КУРСОВОЙ РАБОТЫ

3.1. Общие требования

Системный анализ определенных темой объектов и процессов является целеполагающей основой работы.

Венцом исследования обязаны стать:

- разделы работы, четко решающие каждую из поставленных задач КР;

- выводы по состоянию исследуемого вопроса (полученным результатам);

- рекомендации и предложения по развитию исследований в данном направлении (задачи на будущее).

Общие требования к оформлению КР:

Структура и содержание работы должны соответствовать выбранной теме. Тема – это наикратчайшая форма предъявления содержания всей работы, отражающая её сущность. Выбор тем широк, но необходимо аргументировать, обосновать постановку исследования и выделить цель работы. Тема работы может быть развита в следующей КР, однако во введении необходимо ясно указать: что нового выполняется в данной работе. В соответствии с выбранной темой формулируется цель и задачи работы, например:

- изучение цели, задач и методов психологии безопасности персонала в организации;

- рассмотрение методов противодействия угрозе покушения или психологического давления на сотрудников организации.

Во введении должна быть дана оценка современного состояния решаемой научно-технической проблемы, обоснована необходимость проведения этой работы, показана актуальность темы. Введение должно содержать основание и исходные данные для разработки темы. Во введении должны быть показаны цели и задачи работы. Не допускается введение составлять как аннота-

цию и не рекомендуется во введение включать таблицы и рисунки.

Основная часть в общем случае может состоять из теоретических (научно-исследовательских) и расчетных разделов. В зависимости от особенностей работы отдельные разделы допускается исключать, а также вводить новые разделы в соответствии с требованиями задания на работу.

Заключение должно содержать:

- краткие выводы по выполнению задания на КР;
- результаты оценки полноты решений поставленных задач;
- предложения по использованию, включая внедрение.

Список литературы должен содержать сведения об источниках, использованных при составлении расчетно-пояснительной записки. Их число должно варьироваться в пределах от 15 до 20 указаний. Слишком большой список литературы не всегда может оправдать свой объем, чаще он просто загромождает КР. Сведения об источниках приводят в соответствии с требованиями ГОСТ 7.1.

3.2. Правила оформления текстовых документов

Текст выполняется с использованием компьютера и принтера – в редакторе Microsoft Word: шрифт Times New Roman, размер – 14, цвет шрифта – черный, междустрочный интервал – полуторный, отступ первой строки (абзацный отступ) 1,25 см, выравнивание текста – по ширине, расстановка переносов по тексту – автоматическая, в режиме качественной печати.

Текст следует печатать, соблюдая следующие размеры полей: левое – 20 мм, правое – 10 мм, верхнее – 20 мм, нижнее – 20 мм.

Страницы должны быть заполнены текстом не менее чем на 1/3 часть.

Текст документа должен быть кратким, четким и не допускать различных толкований.

В тексте документов должны использоваться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии – общепринятые в научно-технической литературе.

Если в текстовых документах в большом количестве используется специальная терминология, то в содержание документа добавляют перечень принятых терминов с соответствующими разъяснениями. Перечень располагают перед списком литературы.

В тексте документов не допускается (по ГОСТ 2.105):

– применять для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), а также иностранные слова и термины при наличии равнозначных слов и терминов в русском языке;

– использовать в тексте математический знак минус (-) перед отрицательными значениями величин. Вместо математического знака (-) следует писать слово «минус»;

– применять без числовых значений математические знаки, например, > (больше), < (меньше), = (равно), ≥ (больше или равно), ≤ (меньше или равно), ≠ (не равно), а также знаки № (номер), % (процент);

– применять обозначения нормативных документов (ГОСТ, ТУ, СТП) без регистрационного номера;

– применять обороты разговорной речи, техницизмы, профессионализмы;

– применять производные словообразования.

Если в тексте документа принята особая система сокращения слов или наименований, то расшифровку дают непосредственно в тексте при первом упоминании. Например «…защита информации (ЗИ)», после чего в дальнейшем можно пользоваться сокращением ЗИ.

Текст документа разделяют на разделы, подразделы, которые, в свою очередь, могут состоять из пунктов и подпунктов.

Разделы, подразделы должны иметь заголовки. Заголовки следует печатать с прописной буквы без точки в конце, не под-

черкивая. Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

Между заголовком раздела и подраздела не должно быть пустых строк. Расстояние между заголовком раздела (подраздела) и текстом или пунктом должно быть равно 1 строке.

Каждый раздел текстового документа следует начинать с нового листа.

Разделы должны иметь порядковые номера в пределах текстового документа, обозначенные арабскими цифрами без точки и записанные с абзацного отступа. Подразделы должны иметь нумерацию в пределах каждого раздела. В конце номера подраздела точка не ставится. Разделы, как и подразделы, могут состоять из одного или несколько пунктов.

Если раздел или подраздел состоит из одного пункта, то пункт не нумеруется.

Если текстовый документ не имеет подразделов, то нумерация пунктов должна быть в пределах каждого раздела и номер пункта должен состоять из номеров раздела и пункта, разделенных точкой. В конце номера пункта точка не ставится, например:

1 Социотехнические основы информационной безопасности личности

1.1 }
1.2 } **Нумерация подразделов первого раздела документа**

2. Угрозы Социотехнической безопасности личности

2.1 }
2.2 } **Нумерация подразделов второго раздела документа**

Если подразделы состоят из пунктов, то нумерация пунктов должна быть в пределах подраздела и номер пункта должен состоять из номеров радела, подраздела и пункта, разделенных точками, например:

3 Манипуляция человеческим сознанием

3.1 Манипулятивные возможности СМИ

3.1.1 }
3.1.2 } **Нумерация пунктов первого подраздела третьего раздела текстового документа**
3.1.3 }

Если текст подразделяется только на пункты, они нумеруются порядковыми номерами в пределах текстового документа.

Пункты, при необходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например, 4.2.1.1, 4.2.1.2, 4.2.1.3 и т.д.

Внутри пунктов или подпунктов могут быть приведены перечисления.

Перед каждой позицией перечисления следует ставить дефис или, при необходимости, ссылки в тексте документа на одно из перечислений, строчную букву, после которой ставится скобка. Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

Пример

а) _____;
б) _____;
1)_____;
2)_____.

Каждый пункт, подпункт и перечисление записывают с абзацного отступа.

Содержание включают в общее количество листов текстовых документов.

Слово «Содержание» записывают в виде заголовка (посередине первой строки листа симметрично тексту) с прописной буквы. Наименования, включенные в содержание, записывают строчными буквами, начиная с прописной буквы.

Введение и заключение не нумеруются как разделы.

3.3. Правила нумерации страниц

Страницы текстовых документов следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту. Номер страницы проставляют в центре нижней части листа без точки.

Титульный лист включают в общую нумерацию страниц текстовых документов. Номер страницы на титульном листе не

проставляют.

Иллюстрации и таблицы, расположенные на отдельных листах, содержание, введение, заключение, приложения включают в общую нумерацию страниц текстовых документов.

Иллюстрации и таблицы на листе формата А3 учитывают как одну страницу.

3.4. Правила оформления иллюстраций

Количество иллюстраций (чертежи, графики, схемы, диаграммы, фотоснимки) должно быть достаточным для пояснения излагаемого текста. Иллюстрации следует располагать непосредственно после текста, в котором они упоминаются впервые или на следующей странице.

Фотоснимки размером меньше формата А4 должны быть наклеены на стандартные листы белой бумаги. Иллюстрации могут быть цветными. На все иллюстрации, называемые в тексте рисунками, должны быть даны ссылки.

Иллюстрации (за исключением иллюстраций приложений) следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается «Рисунок 1». Слово «Рисунок» располагают посередине строки.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например – Рисунок 1.1.

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст).

Расстояние от текста до рисунка, от рисунка до подрисуночной надписи и подписи под рисунком равно 1 строке.

При ссылках на иллюстрации следует писать:

- «…в соответствии с рисунком 2» при сквозной нумерации;

- «… в соответствии с рисунком 1.2» при нумерации в пределах раздела.

3.5. Оформление таблиц

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Наименование таблиц, при его наличии, должно отражать ее содержание, быть точным, кратким. Наименование следует помещать над таблицей слева, без абзацного отступа в одну строку с ее номером через тире. Например,

Таблица _____ – _____
(номер) название таблицы (при необходимости)

Расстояние от текста до таблицы и от таблицы до последующего текста равно одной строке.

Между наименованием таблицы и самой таблицей не должно быть пустых строк.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией. Если в текстовых документах одна таблица, она должна быть обозначена «Таблица 1».

Допускается нумеровать таблицы в пределах раздела. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой.

На все таблицы должны быть приведены ссылки в тексте документа, при ссылке следует писать «таблица» с указанием ее номера, например: «…в таблице 1».

Таблицу, в зависимости от ее размера, помещают под текстом, в котором впервые дана ссылка не нее, или на следующей странице.

Допускается помещать таблицу вдоль длинной стороны листа текстовых документов.

Таблицу с большим числом строк допускается переносить на другую страницу, помещая одну часть под другой.

При переносе повторяют заголовки столбцов таблицы.

При отсутствии отдельных данных в таблице следует ставить прочерк (тире).

3.6. Приложения

Приложения оформляют как продолжение текстового документа на последующих его листах. Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Приложения, как правило, выполняют на листах формата А4.

Приложениями могут быть, например, графический материал, таблицы большого формата, расчеты, описания аппаратуры и приборов, описания алгоритмов и программ задач, решаемых на ЭВМ и т.д.

Каждое приложение следует начинать с новой страницы, с указанием наверху посередине страницы слова «ПРИЛОЖЕНИЕ» и его обозначения, а под ним в скобках для обязательного приложения пишут слово «обязательное», а для информационного – «рекомендуемое» или «справочное».

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением Ё, З, Й, О, Ч, Ь, Ы, Ъ. Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и O.

В случае полного использования букв русского и латинского алфавитов допускается обозначать приложения арабскими цифрами.

Приложение должно иметь заголовок, который записывают симметрично относительно текста с прописной буквы отдельной строкой.

Если в текстовом документе одно приложение, оно обозначается «ПРИЛОЖЕНИЕ А», а в тексте при ссылках на него пишут «… в соответствии с приложением А».

Текст каждого приложения при необходимости разделяют на разделы, подразделы и пункты, нумеруемые по каждому приложению. Перед номером ставится обозначение этого приложения.

Иллюстрации, таблицы и формулы в приложениях нумеруют в пределах каждого приложения.

В тексте документа на все приложения должны быть даны ссылки. Приложения в содержании располагают в порядке ссылок на них в тексте с указанием их обозначений, заголовков и номеров страниц.

3.7. Типичные ошибки при выполнении курсовой работы

Попытка опереться в изложении на какой-либо один источник, влекущая за собою узость рассмотрения проблемы и сложности обоснования актуальности работы.

Копирование источников без творческого анализа состояния вопроса.

Бессистемное, непоследовательное и неконкретное изложение вопроса без графиков, формул и таблиц, являющихся необходимым атрибутом технических наук.

Стремление объёмным «словоблудием» скрыть несостоятельность работы.

Небрежное оперирование терминами и понятиями.

Использование жаргонов (чаще всего из интернет-материалов) в изложении.

Пренебрежение к лекционному материалу и замечаниям руководителя, нацеливающих автора на выполнение качественной работы.

4. РЕКОМЕНДУЕМЫЕ ТЕМЫ КУРСОВЫХ РАБОТ

Рекомендуемые темы курсовых работ представлены в табл. 6.

Таблица 6

Рекомендуемые темы курсовых работ

Категория	Шаблон атак
1.GatherInformation (Сбор информации)	1.Excavation (Раскопки) 2. Interception (Перехват) 3. Footprinting --- 4. Fingerprinting (Дактилоскопия) 5.Social Information Gathering Attacks (Социально-информационный сбор атак) 6. InformationElicitationviaSocialEngineering (Сбор информации через Социальную Разработку)
2.Deplete Resources (Истощение ресурсов)	1. Flooding (Лавинная рассылка) 2. ExcessiveAllocation (Чрезмерное распределение (или выделение)) 3. ResourceLeakExposure (Воздействие утечки ресурсов) --- 4. SustainedClientEngagement (Длительное клиентское обязательство) 5. Amplification (Усиление) ---
3.Injection (Инъекция)	1. Parameter Injection (Инжекцияпараметра) 2. CodeInclusion (включениекода) 3. ResourceInjection (Инжекцияресурса) 4. CodeInjection (инжекциякода) 5. Command Injection (Инжекция команды)
4. Deceptive Interactions (Обманчивые взаимодействия)	1. PathTraversal (Соедините обход каналом) 2. ContentSpoofing (Содержание, имитирующее) 3. IdentitySpoofing (Идентификационные данные, имитирующие) 4. ResourceLocationSpoofing(Расположение ресурса, имитирующее) 5. Action Spoofing (имитация действия)

Продолжение табл. 6

Категория	Шаблон атак
5.ManipulateTiming andState (Манипулирование сроками получения и состоянием)	1. ForcedDeadlock (Принудительная мертвая блокировка) 2. Leveraging Race Conditions (Усиление условий состязания) 3. LeveragingTime-of-CheckandTime-of-Use (TOCTOU) RaceConditions (Усиление времени проверки и времени использования (TOCTOU) условия состязания) 4. Cross-DomainSearchTiming (Междоменный поиск, рассчитывающий) 5. ManipulatingUserState (Управление пользовательским состоянием)
6. AbuseofFunction-ality (Злоупотребление функциональностью)	1. APIAbuse/Misuse (Злоупотребление/ Неправильное употребление API) 2. TryAllCommonApplicationSwitchesand Options (Попробуйте Все Переключатели Общего применения и Опции) 3. CachePoisoning (Кэш Отравляющий) 4. SoftwareIntegrityAttacks (Атаки Целостности программного обеспечения) 5. FunctionalityMisuse (Неправильное употребление функциональности) 6. Directory Traversal (Обход каталога) 7. AbuseofCommunicationChannels (Злоупотребление Каналами передачи) 8. SocketCapableBrowserPluginsResultIn TransparentProxyAbuse (Снабдите Способный Результат Плагинов Браузерасокетом В Прозрачном Злоупотреблении По доверенности) 9. PassingLocalFilenamestoFunctionsThat Expecta URL (Передача Локальных Имен файлов к Функциям, Которые Ожидают URL) 10. ForcefulBrowsing(Мощный Просмотр) 11. WSDLScanning (Сканирование WSDL)

Продолжение табл. 6

Категория	Шаблон атак
7. Probabilistic Techniques (Вероятностные методы)	1. BruteForce (Грубая сила) 2. ScreenTemporaryFilesforSensitive Information (Экранируйте временные файлы на уязвимую информацию) 3. Fuzzing 4. Manipulating Opaque Client-based Data Tokens (Управление непрозрачными основанными на клиенте маркерами данных)
8. Exploitation of Authentication (Эксплуатацияпроверки подлинности)	1. AuthenticationAbuse (Злоупотребление аутентификации) 2. AuthenticationBypass (Обход аутентификации) 3. ExploitationofSessionVariables, ResourceIDsandotherTrustedCredentials (Эксплуатация Переменных Сеанса, ID Ресурса и других Доверяемых Учетных данных)
9.Exploitation of Authorization (Эксплуатация авторизации)	1. Privilege Escalation (Расширение полномочий) 2. Privilege Abuse (Злоупотребление полномочиями) 3. ExploitingTrustinClient (akaMakettheClientInvisible) (Использование Доверия Клиента (иначе Делают Клиент Невидимым)) 4. Hijacking a privileged process (Угон привилегированного процесса) 5. Catchingexceptionthrow/signalfromprivilegedblock (Ловля исключения бросает/ сигнализирует от привилегированного блока) 6. Hijacking a Privileged Thread of Execution (Угон Привилегированного Потока Выполнения) 7. SubvertCode-signingFacilities (Ниспровергайте средства подписывания кода) 8. Target Programs with Elevated Privileges (Целевые Программы с Поднятыми Полномочиями)

Продолжение табл. 6

Категория	Шаблон атак

10. ManipulateData Structures (Манипулирование структурами данных)	1. BufferManipulation (Буферное манипулирование) 2. AttackthroughSharedData (Атака через совместно используемые данные) 3. IntegerAttacks (Целочисленная атака) 4. PointerAttack (Указательная атака) 5. Accessing/Intercepting/Modifying HTTP Cookies (Доступ/Прерывание/Изменение cookie HTTP)
11. Manipulate Resources (Манипулированиересурсами)	1. InputDataManipulation (Введите Манипулирование данными) 2. ResourceLocationSpoofing(Расположение ресурса, Имитирующее) 3. InfrastructureManipulation (Манипулирование инфраструктурой) 4. FileManipulation (Манипулирование файлом) 5. VariableManipulation (Переменное Манипулирование) 6. Configuration/Environmentmanipulation (Манипулирование конфигурацией/Средой) 7. AbuseofTransactionDataStructure (Злоупотребление Структурой Данных транзакции) 8. AuditLogManipulation (Контрольное Манипулирование Журналом) 9. SchemaPoisoning (Схема, Отравляющая) 10. ProtocolManipulation (Манипулирование протоколом) 11. Accessing/Intercepting/Modifying HTTP-Cookies (Доступ/Прерывание/ Изменение Cookie HTTP) 12. Contaminate Resource (Засорение ресурса)
12.AnalyzeTarget (Анализ цели)	1. Reverse Engineering (Инженерныйанализ) 2. Cryptanalysis (Криптоанализ)
13. GainPhysical Access (Получениефизическогодоступа)	1. BypassingPhysicalSecurity (Обход физической безопасности) 2. PhysicalTheft (Физическое воровство)

Окончание табл. 6

Категория	Шаблон атак

14.MaliciousCodeExecution (Выполнение вредоносного кода)	1. TargetedMalware(Предназначенное вредоносное программное обеспечение)
15.Alter System Components (Изменитькомпонентысистемы)	1. Hacking Hardware Devices or Components(Взламывание устройств или компонентов) 2. Physical Destruction of Device or Component (Физическое разрушение устройства или компонента)
16. Manipulate SystemUsers (Манипулировать системными пользователями)	1. Target Influence via Social Engineering (Целевое Влияние через Социальную Разработку)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации от 12 декабря 1993 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

2. Резолюция Генеральной Ассамблеи ООН 56/19 от 7 января 2002 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (по докладу Первого комитета (A/56/533) [Электронный ресурс] – Режим доступа: http: //www.garant.ru

3. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) [Электронный ресурс] – Режим доступа: http: //www.garant.ru

4. Окинавская Хартия глобального информационного общества от 22 июля 2000г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

5. Соглашение об основных принципах военно-технического сотрудничества между государствами-участниками Договора о коллективной безопасности от 15 мая 1992 г. (Москва, 20 июня 2000 г.) [Электронный ресурс] – Режим доступа: http: //www.garant.ru

6. Налоговый Кодекс Российской Федерации. Часть первая. 31 июля 1998 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

7. Уголовный Кодекс Российской Федерации от 13 июня 1996 г. // [Электронный ресурс] – Режим доступа: http: //www.garant.ru

8. Гражданский Кодекс Российской Федерации. Часть вторая. 22 декабря 1995 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

9. Гражданский Кодекс Российской Федерации. Часть первая. 21 октября 1994 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

10. Основы законодательства Российской Федерации об охране здоровья граждан № 5487-1 от 22 июля 1993 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

11. Федеральный закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27 июля 2006 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

12. Федеральный закон «О коммерческой тайне» № 98-ФЗ от 29 июля 2004 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

13. Федеральный закон «О связи» № 126-ФЗ от 7 июля 2003 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

14. Федеральный закон «О техническом регулировании» № 184-ФЗ от 27 декабря 2002 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

15. Федеральный закон «О несостоятельности (банкротстве)» № 127-ФЗ от 26 октября 2002 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

16. Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» № 63-ФЗ от 31 мая 2002 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

17. Федеральный закон «Об электронной цифровой подписи» № 1-ФЗ от 10 января 2002 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

18. Федеральный закон «О государственной регистрации юридических лиц и индивидуальных предпринимателей» № 129-ФЗ от 8 августа 2001 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

19. Федеральный закон «Об аудиторской деятельности» № 119-ФЗ от 7 августа 2001 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

20. Федеральный закон «О государственном земельном кадастре» № 28-ФЗ от 2 января 2000 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

21. Федеральный закон «О наркотических средствах и психотропных веществах» № 3-ФЗ от 8 января 1998 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

22. Федеральный закон «Об актах гражданского состояния» № 143-ФЗ от 15 ноября 1997 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

23. Федеральный закон «О государственной регистрации прав на недвижимое имущество и сделок с ним» № 122-ФЗ от 21 июля 1997 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

24. Федеральный закон «Об участии в международном информационном обмене» № 85-ФЗ от 4 июля 1996 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

25. Федеральный закон «О рынке ценных бумаг» № 39-ФЗ от 22 апреля 1996 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

26. Федеральный закон «О ратификации Устава и Конвенции Международного союза электросвязи» № 37-ФЗ от 30 марта 1995 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

27. Федеральный закон «О библиотечном деле» № 78-ФЗ от 29 декабря 1994 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

28. Закон Российской Федерации «О государственной тайне» № 5485-1 РФ от 21 июля 1993 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

29. Закон Российской Федерации «Об авторском праве и смежных правах» № 5351-I от 9 июля 1993 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

30. Закон Российской Федерации «О правовой охране топологий интегральных микросхем» № 3526-I от 23 сентября 1992 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

31. Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз дан-

ных» № 3523-I от 23 сентября 1992 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

32. Патентный закон Российской Федерации № 3517-I от 23 сентября 1992 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

33. Закон Российской Федерации «О средствах массовой информации» № 2124-I от 27 декабря 1991 г. [Электронный ресурс] – Режим доступа: http: //www.garant.ru

34. Гражданское право: В 4 т. Т.1. Общая часть [Текст]: учебник / под ред. Е. А. Суханова. – 3-е изд., перераб. и доп. – М.: Издательство Волтерс Клувер, 2004. – 720 с.

35. Гражданское право: В 2 т. Т.2. Полутом 1 [Текст]: учебник / под ред. Е. А. Суханова. – 2-е изд., перераб. и доп. – М.: Издательство Волтерс Клувер, 2004. – 704 с.

36. Ионин, Л. Г. Философия и методология эмпирической социологии [Текст]: учеб. пособие / Л. Г. Ионин. – М.: «Книга сервис», 2004. – 366 с.

37. Кравченко, А. И. Социология [Текст]: учебник / А. И. Кравченко.–М.: Академический Проект, 2002. – 508 с.

38. Криминология [Текст]: учеб. пособие / Под общ. ред. Ю.Ф. Кваши. – Ростов-на-Дону: Феникс, 2002. – 704 с.

39. Платонов, Д. И. Уголовное право Российской Федерации. Общая часть [Текст]: учеб. пособие / Д. И. Платонов. – М.: «Книга сервис», 2003. – 112 с.

40. Протасов, В. Н. Что и как регулирует право [Текст]: учеб. пособие / В. Н. Протасов. – М.: Юристъ, 1995.– 95 с.

41. Тедеев, А. А. Информационное право [Текст]: учебник / А. А. Тедеев. – М.: Издательство Эксмо, 2005. – 464 с.

42. Хорошилов, А. В. Мировые информационные ресурсы [Текст]: учеб. пособие / А. В. Хорошилов. – СПб.: Питер, 2004. – 176 с.

43. Червонюк, В. И. Теория государства и права [Текст]: учеб. пособие / В. И. Червонюк. – М.: Инфра-М, 2003. – 256 с.

44. Абульханова, К. А. Психология и сознание личности: Проблемы методологии, теории и исследования реальной личности [Текст] / К. А. Абульханова. – М.: Московский психолого-социальный институт, 1999. – 224 с.

45. Вержбицкий, В. М. Численные методы: линейная алгебра и нелинейные уравнения [Текст] / В. М. Вержбицкий. – М.: «Высшая школа», 2000. – 266 с.

46. Войниканис, Е. А. Информация. Собственность. Интернет. Традиция и новеллы в современном праве [Текст] / Е. А. Войниканис, М.В. Якушев. – М.: Волтерс Клувер, 2004. – 163 с.

47. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Текст] / А. Г. Волеводз. – М.: ООО Издательство «Юрлитинформ», 2002. – 496 с.

48. Волобуев, С. В. Философия безопасности социотехнических систем [Текст] / С. В. Волобуев. – М.: «Вузовская книга», 2002. – 360 с.

49. Завидов, Б. Д. Обычное мошенничество и мошенничество в сфере высоких технологий [Текст]: практическое пособие / Б. Д. Завидов. – М.: Издательство «Приор», 2002. – 32 с.

50. Зинченко, С. А. Проблемы объектов гражданских прав [Текст] / С. А. Зинченко, В. А. Лапач, Д. Ю. Шапсугов. – Ростов-на-Дону: Издательство СКАГС, 2001. – 432 с.

51. Каптерев, А. И. Информатизация социокультурного пространства [Текст] / А. И. Каптерев. – М.: Фаир-Пресс, 2004. – 512 с.

52. Лапач, В. А. Система объектов гражданских прав: Теория и судебная практика [Текст] / В. А. Лапач. – СПб.: Изд-во «Юридический центр Пресс», 2002. – 526 с.

53. Ледбитер, Ч. Астральный план [Текст]: пер. с англ. / Ч. Ледбитер. – М.: «Амрита-Русь», 2004. – 128 с.

54. Лунгу, К. Н. Линейное программирование [Текст] / К. Н. Лунгу. – М.: Высшая школа, 2005. – 128 с.

55. Манойло А.В. Государственная политика в условиях информационно-психологической войны [Текст] / А. В.

Манойло, А. И. Петренко, Д. Б. Фролов. – М.: Горячая линия - Телеком, 2003. – 541 с.

56. Международная защита прав человека с использованием некоторых международно-правовых механизмов [Текст] / К. А. Москаленко, А. Н. Канин, Э. Г. Зусманович и др.; под. ред. Центра содействия международной защите. – М.: Издательский дом «Галерия», 2001. – 160 с.

57. Могилевский, В. Д. Методология систем [Текст] / В. Д. Могилевский. – М.: «Экономика», 1999. – 251 с.

58. Новосельцев, В. И. Системная конфликтология [Текст] / В. И. Новосельцев. – Воронеж: Издательство «Кварта», 2001. – 176 с.

59. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность [Текст] / С. А. Петренко. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

60. Петросян, Л.А. Теория игр [Текст] / Л. А. Петросян, Н. А. Зенкевич, Е. А. Семина. – М.: Высшая школа, 1998. – 304 с.

61. Почепцов, Г. Г. Психологические войны [Текст] / Г. Г. Почепцов. – М.: Издательство «Рефл-бук», 2000. – 528 с.

62. Пригожин, И. Порядок из хаоса [Текст]: пер. с англ. / И. Пригожин, И. Стенгерс. – М.: Прогресс, 1986. – 431 с.

63. Прокофьев, В. Ф. Тайное оружие информационной войны [Текст] / В. Ф. Прокофьев. – М.: Синтег, 1999. – 152 с.

64. Андреев, Б. В. Расследование преступлений в сфере компьютерной информации [Текст] / Б. В. Андреев, П. Н. Пак, В. П. Хорст. – М.: Издательство «Юрлитинформ», 2001. – 152 с.

65. Расторгуев, С. П. Введение в формальную теорию информационной войны [Текст] / С. П. Расторгуев. – М.: Вузовская книга, 2002. – 120 с.

66. Расторгуев, С. П. Философия информационной войны [Текст] / С. П. Расторгуев. – М.: Московский психолого-социальный институт, 2003. – 496 с.

67. Селигмен, Б. Основные течения современной экономической мысли [Текст]: пер. с англ. / Б. Селигмен.– М.: «Прогресс», 1993. – 466 с.

68. Системные закономерности и системная оптимизация [Текст] / И. В. Прангишвили, В. Н. Бурков, И. А. Горгидзе, Г. С. Джавахадзе, Р. А. Хуродзе– М.: Синтег, 2004. – 208 с.

69. Прангишвили, И. В. Системные законы и закономерности в электродинамике, природе и обществе [Текст] / И. В. Прангишвили, Ф. Ф. Пащенко, Б. П. Бусыгин – М.: Наука, 2001. – 525 с.

70. Снытников, А. А. Обеспечение и защита права на информацию [Текст] / А. А. Снытников, Л.В. Туманова. – М.: Городец-издат, 2001. – 344 с.

71. Хозиков, В. И. Информационное оружие [Текст] / В. И. Хозиков. – М.: Издательство «Олма-Пресс Образование», 2003 – 480 с.

72. Чалдини, Р. Психология влияния [Текст]: пер. с англ. / Р. Чалдини. – СПб.: Издательство «Питер», 2003. – 288 с.

73. Шамраев, А. В. Правовое регулирование информационных технологий. Анализ проблем и основные документы [Текст] / А. В. Шамраев. – М.: Министерство иностранных дел Российской Федерации, 2003. – 1011 с.

74. Сенчищев, В. И. Объект гражданского правоотношения. Общее понятие [Текст] / В. И. Сенчищев // Актуальные вопросы гражданского права. – 1998. – С. 109-160.

75. Стрельцов, А. А. Информация как объект исследования в естественных, технических и социальных науках [Текст] / А. А. Стрельцов // Влияние информационных технологий на национальную безопасность: сб. рабочей группы Консорциума «». – М.: Московский государственный университет, 2002. – С. 6-19.

76. Барабанщикова, Л. М. Структура права собственности в российском гражданском праве [Текст] / Л. М. Барабанщиков // Юридический мир. – 2003. – № 4. – С. 19-24.

77. Дозорцев, В. А. Развитие законодательства о правах на результаты интеллектуальной деятельности [Текст] / В. А. Дозорцев // Экономика и жизнь. – 1996. – № 40. – С. 4-10.

78. Клишина, А. Коллизионные вопросы использования коммерческой тайны [Текст] / А. Клишина // Интеллектуаль-

ная собственность: Промышленная собственность. – 2005. – № 1. – С.48-56.

79. Копылов, В. А. О систематизации и кодификации информационного законодательства и праве собственности на объекты информационных отношений [Текст] / В. А. Копылов // Науч.-техн. информ. Сер. 1. Организация и методика информационной работы. – 2002. – № 5. – С. 1-13.

80. Курило, А. П. О проблеме компьютерной безопасности [Текст] / А. П. Курило // Научно-техническая информация. Сер. 1. Орг. и методика информ. работы. – 1993. – № 8. – С .7-10.

81. Лобанов, Г. Информация как объект гражданских правоотношений [Текст] / Г. Лобанов // Бизнес адвокат. – 1998. – № 6. – С. 11-19.

82. Селиванов, Н. Проблемы борьбы с компьютерной преступностью [Текст] / Н. Селиванов // Законность. – 1993. – № 8. – С. 36-37.

83. Семилетов, С .И. Информация как особый нематериальный объект права [Текст] / С. И. Семилетов //Государство и право. – 2000. – № 5. — С. 67-68.

84. Сурнин, В. Информация и информационно-обменные процессы [Текст] / В. Сурнин // Стандарты и качество. – 2005. – № 11. – С. 83-85.

85. Фролов, Д. Б. Новая система страха – кибертерроризм [Текст] / Д. Б. Фролов, Е. В. Старостина // Безопасность информационных технологий. – 2004. – № 2. – С. 18-24.

86. Шишмарева, Е. В. Общие признаки информации, составляющей коммерческую тайну [Текст] / Е. В. Шишмарева // Журнал российского права. – 2004. – № 9. – С. 73-80.

87. Южанин, Н. В. Вещное и обязательственное право (философско-правовой очерк) [Текст] / Н. В. Южанин // Юрист. – 2004. – № 6. – С. 2-13.

88. Ястребов, О. В. Право собственности на информацию [Текст] / О. В. Ястребов // Юрист. – 2004. – № 6. – С. 13-17.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовым работам по дисциплине
«Социотехнические основы
информационной безопасности»
для студентов специальностей
090301 «Компьютерная безопасность»,
090302 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составители:
Остапенко Александр Григорьевич
Бурса Максим Васильевич

В авторской редакции

Подписано к изданию 20.04.2015.
Уч.-изд. л. 4,2.

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14