УДК 002:34+004.056.5
ББК 32.82
Ж 850

Введение

Современный мир совершает переход из XX – «энергетического» века в XXI век, который со всей определенностью можно назвать «информационным». И сегодня на смену индустриальному этапу общественного развития приходит эволюционная фаза, названная информатизацией, при которой все социально-экономические структуры общества преобразуются таким образом, чтобы обеспечить этим структурам и обществу в целом наиболее эффективное и динамичное развитие на основе максимально полною использования имеющихся информационных ресурсов. Традиционные материальные ресурсы постепенно утрачивают свое первоначальное значение, а им на смену приходят информационные ресурсы, которые со временем не убывают, а неуклонно растут. Информация как предмет труда становится все в большей степени стратегическим ресурсом общества, ею движущей производительной силой.

В условиях информатизации общества особую ценность обретают люди - носители знаний, наилучшие передатчики технологической информации и передовою опыта. Для их эффективного участия в информационных процессах создается мощнейшая инфраструктура средств компьютерной и телекоммуникационной техники, изменяющая не только процесс и характер трудовой деятельности, но и сам образ жизни, систему ценностей человека. В настоящее время хорошо налаженная распределенная есть информационно-вычислительных комплексов способна сыграть такую же

роль в современном обществе, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые.

Современные информационные технологии приобретают глобальный характер, охватывая все сферы жизнедеятельности человека, формируя информационное единство всей человеческой цивилизации. С помощью глобальной вычислительной сети Интернет объединяются и перемещаются на любые расстояния гигантские объемы информации, обеспечивается доступ многочисленных пользователей, расположенных на практически неограниченной территории к информационным ресурсам всего мирового сообщества.

Таким образом, ныне информация превратилась из абстрактного понятия в едва ли не самый ценный объект во Вселенной и ход всех значимых событий в науке, коммерции, социуме связан с процессами производства и владения информацией. С другой стороны, **информационная безопасность (ИБ)** – сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ базис – ***концептуально-методологические основы ИБ***.

1. Основы системного понимания информационной безопасности

Известно, что научно-технический потенциал государства зависит от уровня информационного обеспечения труда ученых, инженеров, наличия систем автоматизации проектирования (САПР), автоматизированных систем научных исследований (АСНИ), средств осуществления вычислительных экспериментов, телеконференций и т.д. Низкий уровень этого обеспечения наряду с экономическим фактором в настоящее время не позволяет проводить исследования на передовых рубежах науки и техники и является одной из основных причин утечки «мозгов» из нашей страны.

В военном деле, например, наступает новый, постядерный этап развития. Эффективность современного оружия все больше определяется не столько огневой мощью, сколько степенью информационной обеспеченности. Информатизация армии стала приоритетной задачей военно-технической политики государства. В содержании военных действий возросла значимость информационно-технического противоборства. Превосходство в степени информированности - непременное условие победы в воздушном, морском и сухопутном бою (сражении, операции), залог успеха в противовоздушной обороне. Об этом свидетельствует опыт вооруженных конфликтов и локальных войн современности.

Возрастание роли информационно-технической борьбы стирает границу между войной и миром. Вооруженные силы ряда государств находятся в постоянном информационном противоборстве, а военная информатика и в мирное время решает задачи, характерные для войны. В Пентагоне, например, руководствуются лозунгом «Радиоэлектронная война никем не объявляется, никогда не прекращается, ведется скрытно и не знает границ в пространстве и времени». Началась борьба за владение компьютерными сетями. Обмен «информационными ударами» становится все опаснее для судеб мира, поскольку их эффективность быстро возрастает.

Впервые в России понятие «информационная безопасность» было введено в 1990 г. в парламентской комиссии академика Ю.А. Рыжова, которая занималась разработкой концепции национальной безопасности страны. С тех пор созданы соответствующие структуры в Правительстве РФ, в Администрации Президента РФ, в Совете безопасности РФ, которые занимаются напрямую этими вопросами. В 1996 г. был создан парламентский подкомитет по информационной безопасности. Вопросы информационной безопасности заняли прочную строчку во всех посланиях Президента РФ, они вошли в Концепции по национальной безопасности, утвержденные 17 декабря 1997 г. и 10 января 2000 г.

Несмотря на обилие структур (по отдельным оценкам только в государственных информационно-аналитических службах и ситуационных центрах работает более 15 тыс. человек), как следует из Послания Президента РФ по национальной безопасности (13.06.1996 г.), одной из основных угроз для России в информационной сфере является «отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам». Эта угроза актуальна и сегодня и имеет следующие характеристики:

- отсутствие единого правового поля, когда заявленный в Конституции РФ приоритет интересов личности и общества нередко подменяется в законах приоритетом интересов ведомств, а законодательство субъектов федерации зачастую не соответствует федеральному уровню, а подзаконные акты по-прежнему являются основой для произвола чиновников;

- отсутствие единой системы отбора информации, подготовки и принятия эффективных решений на высшем уровне;

- отсутствие должного взаимодействия между существующими структурами обеспечения безопасности, когда ведомства порой подменяют государственные интересы узковедомственными и вступают в противостояние в борьбе за усиление своих полномочий;

- отсутствие системы эффективного контроля за обеспечением безопасности как со стороны вышестоящих государственных структур, так и со стороны общества и граждан, в силу чего нередко даже правильные и необходимые решения не выполняются.

Исходя из того, что информационная безопасность в начале третьего тысячелетия выходит на первое место в системе национальной безопасности, формирование и проведение единой государственной политики в этой сфере требует приоритетного рассмотрения.

Сегодня сложились две основные тенденции в органах государственной власти в определении понятия и структуры информационной безопасности. Представители *гуманитарного направления*

связывают информационную безопасность только с институтом тайны. Представители *силовых структур* предлагают распространить сферу информационной безопасности практически на все вопросы и отношения в информационной сфере, по сути, отождествляя информационную безопасность с информационной сферой. Истина, как всегда, лежит посредине.

В настоящее время очень популярен афоризм ***«кто владеет информацией, тот владеет миром»***. Как известно, на заре начала космической эры известный американский журналист и писатель Т. Вольфе приводит следующее высказывание Председателя подкомитета по боевой готовности сенатор Л. Джонсона (впоследствии президент США) по поводу мотивов США в соревновании с Советским Союзом в области космических исследований: «Римская империя контролировала мир потому, что сумела построить дороги. Затем, когда началось освоение морских пространств, Британская империя доминировала в мире, так как имела корабли. В век авиации мы были могущественны, поскольку имели в своем распоряжении самолеты. Сейчас коммунисты захватили плацдарм в космосе».

Бывший вице-президент, а впоследствии президент США Линдон Б. Джонсон очень много занимался американской космической программой и его формула ***«кто владеет космосом – тот владеет всем миром»*** была воспринята политическим и военным руководством, а также всей американской общественностью как руководство к практическим действиям по совершенствованию военных возможностей Соединенных Штатов Америки. Этот девиз стал основным для американских военных стратегов не только в начале 60-х годов, но и сохранил свою актуальность на современном этапе исторического развития земной цивилизации.

В современном мире, когда формируется и развивается информационное общество, когда разворачивается глобальная информационная война афоризм «кто владеет информацией, тот владеет миром» является не менее актуальным. Кроме того, в настоящее время успех

военных действий на суше, в воздухе и на море, в равной степени, как и предотвращение войны, военно-политических кризисов или вооруженных конфликтов существенно зависят от эффективности использования ***космической информации***. Поэтому целью обеспечения национальной (военной, информационной, экологической и др.) безопасности с использованием космических систем различного целевого назначения является, прежде всего, разработка и эффективное использование органами государственного управления Российской Федерации *комплексной информационной системы сбора, хранения, обработки, преобразования, передачи и реализации полученной космической информации.* Все это убедительно говорит в пользу использования результатов космической деятельности в интересах обеспечения национальной безопасности, а также ее основных составных частей: военной, информационной, экологической и др. безопасности государства.

Таким образом, ***информационная безопасность*** – сравнительно молодая, быстро развивающаяся область информационных технологий, для успешного освоения которой важно с самого начала усвоить современный базис, согласованный с другими ветвями информационных технологий. И успех в области информационной безопасности может принести только системный, комплексный подход.

Словосочетание *«информационная безопасность»* в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин *информационная безопасность* используется в *широком смысле*. Имеется в виду «состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

Необходимо отметить, что информационные воздействия опасны (или полезны) не столько сами по себе, сколько тем, что «запускают» мощные вещественно-энергетические процессы, управляют ими. Суть влияния информации как раз и заключается в ее способности «запускать» и контро-

лировать вещественно-энергетические процессы, параметры которых на много порядков выше самой информации.

С другой стороны, термин *информационная безопасность* часто используется в *узком смысле*, так, как это принято, например, в англоязычной литературе, т.е. под *информационной безопасностью* понимается з*ащищенность* информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*. Далее мы поясним, что следует понимать под *поддерживающей инфраструктурой*. Заметим лишь, что ***защита информации*** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Системный подход к информационной безопасности требует определения ее *субъектов*, *средств* и *объектов*, *источников опасности*, *направленности опасных информационных потоков* и *принципов обеспечения информационной безопасности* (рис. 1).

Объектами опасного информационного воздействия и, следовательно, информационной безопасности могут быть: сознание, психика людей; информационно-технические системы различного масштаба и назначения.

Субъектами информационной безопасности следует считать те органы и структуры, которые занимаются ее обеспечением.

Средства обеспечения информационной безопасности - это средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д.

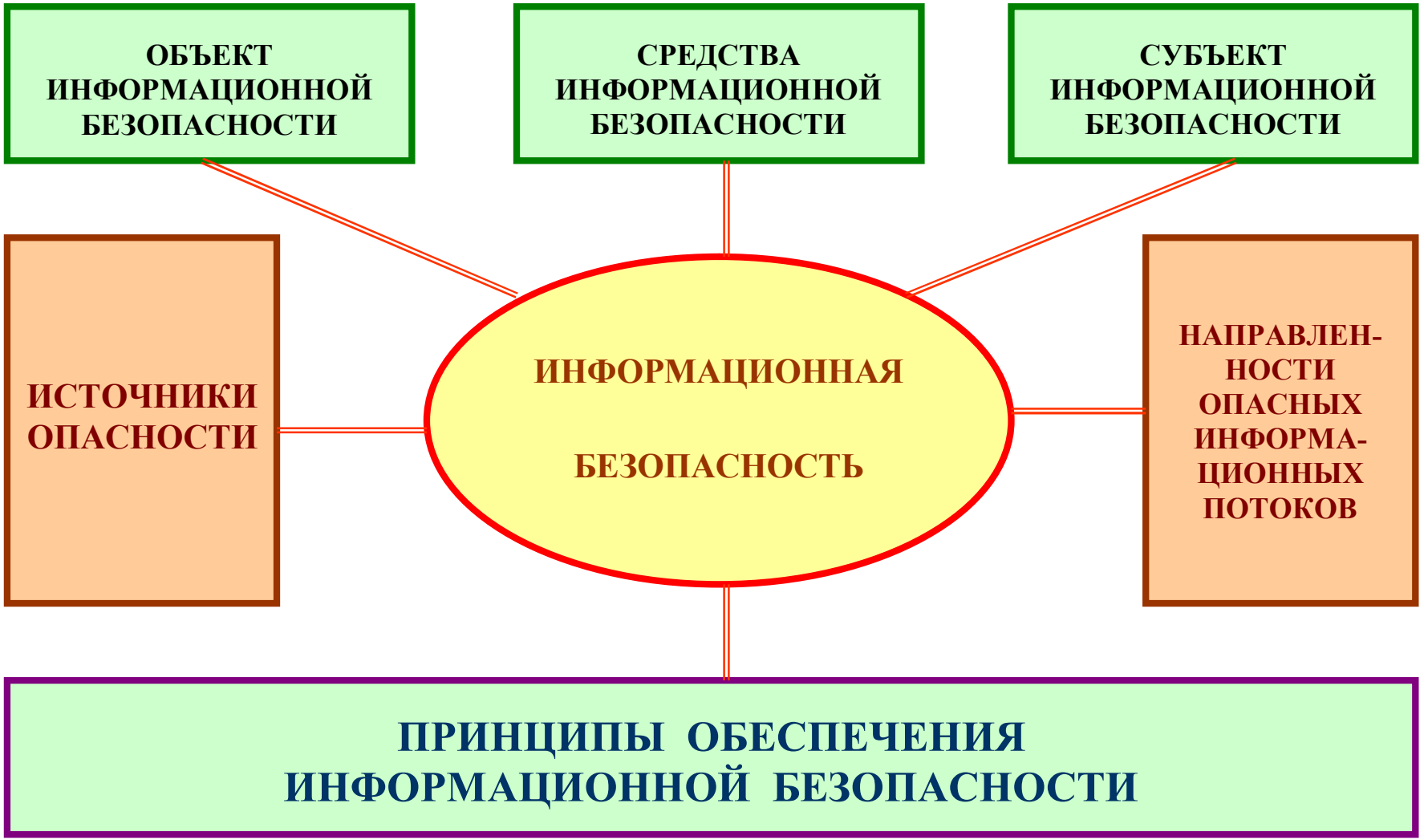

Рис. 1. Системное понимание информационной безопасности

Источники информационных опасностей могут быть естественными (объективными) и умышленными. Первые возникают в результате непреднамеренных ошибок и неисправностей, случайных факторов, стихийных бедствий и др.

Известно, например, что системы ПВО периодически выдают ложные сигналы тревоги из-за разнообразных технических сбоев, но по этим сигналам приводятся в высокую степень боеготовности стратегические ракеты, самолеты - носители ядерного оружия.

Умышленные информационные воздействия осуществляются сознательно и целенаправленно. При этом часто используются средства массовой информации, радиоэлектронной борьбы (РЭБ), специальные программные средства для компьютеров. Они настолько эффективны, что их можно выделить как новый класс оружия - информационный.

Опасные информационные воздействия следует разделить на два вида.

Первый связан с утратой ценной информации, что либо снижает эффективность собственной деятельности, либо повышает эффективность деятельности противника, конкурента.

Если объектом такого воздействия является сознание людей, то речь идет о разглашении государственных тайн, вербовке агентов, специальных мерах и средствах для подслушивания, использовании детекторов лжи, медикаментозных, химических и других воздействиях на психику человека с целью заставить его развязать язык или забыть что-либо. Безопасность от информационного воздействия данного вида обеспечивают органы цензуры, контрразведки и другие субъекты информационной безопасности.

Если же источником информации служат технические системы, то речь идет уже о технической разведке, или шпионаже (перехват телефонных разговоров, радиограмм, сигналов других систем коммуникации), проникновении в компьютерные сети, банки данных. Деятельностью подобного рода занимается, например, агентство национальной безопасности США, затрачивая на это десятки млрд. долларов в год. Противодействуют технической раз-

ведке органы контрразведки, а также структуры, ведающие теорией и практикой защиты компьютерных средств, систем связи.

Второй вид информационного воздействия связан с внедрением негативной информации, что может не только привести к опасным ошибочным решениям, но и заставить действовать во вред, даже подвести к самоубийству, а общество - к катастрофе. Информационную безопасность этого вида должны обеспечивать специальные структуры информационно-технической борьбы. Они нейтрализуют акции дезинформации, пресекают манипулирование общественным мнением, противодействуют РЭБ, ликвидируют последствия компьютерных атак.

К *принципам обеспечения информационной безопасности* можно отнести: законность, баланс интересов личности, общества и государства, комплексность, системность, интеграцию с международными системами безопасности, экономическую эффективность и т.д.

Заметим, что рассмотрение информационной безопасности с позиций системного подхода позволяет увидеть отличие научного понимания этой проблемы от обыденного. В повседневной жизни информационная безопасность понимается лишь как необходимость борьбы с утечкой закрытой (секретной) информации, а также с распространением ложных и враждебных сведений. Осмысления новых информационных опасностей, особенно технического плана, в обществе еще не произошло.

Таким образом, правильный с методологической точки зрения подход к проблемам *информационной безопасности* начинается с выявления *субъектов информационных отношений* и *интересов этих субъектов*, связанных с использованием информационных систем (ИС). *Угрозы информационной безопасности* – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с *информационной безопасностью*, для разных категорий субъектов может существенно различаться. Для

иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «пусть лучше все сломается, чем враг узнает хоть один секретный бит», во втором – «да нет у нас никаких секретов, лишь бы все работало».

2. *Информационная безопасность* не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. *Субъект информационных отношений* может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин *«компьютерная безопасность»* (как эквивалент или заменитель ИБ) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на «горчичнике», прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Развитие и внедрение в различные сферы жизни общества новых информационных технологий, как и любых других научно-технических достижений, не только обеспечивают комфортность, но и нередко несут опасность. Сегодня можно выделить следующие наиболее существенные группы информационно-технических опасностей, обусловленных достижениями научно-технического прогресса.

Первая группа связана с бурным развитием нового класса оружия - информационного, которое способно эффективно воздействовать и на психику, сознание людей, и на информационно-техническую инфраструктуру общества и армии. В настоящее время создано много новых средств воздействия на психику людей, управления их поведением.

С другой стороны, в последние годы происходят революционные перемены в развитии средств радиоэлектронного противодействия. И их возможности достаточно известны. Главное направление прогресса в электронике - компьютеризация. Поэтому особенно быстро и с поразительными успехами разрабатываются методы воздействия на компьютерные системы. Вполне очевидно, что соответствующие службы развитых в области информатики государств ведут подготовку к

«компьютерной войне», разрабатывают и апробируют способы, приемы воздействия на компьютерные системы.

Вторая группа информационно-технических опасностей для личности, общества, государства - это новый класс социальных преступлений, основанных на использовании современной информационной технологии (махинации с электронными деньгами, компьютерное хулиганство и др.). По мнению специалистов, компьютер становится самым многообещающим орудием преступления.

Третья группа информационно-технических опасностей - электронный контроль за жизнью, настроениями, планами граждан, политических организаций. Правящие круги не только используют подслушивание телефонных разговоров, но и осуществляют контроль за перепиской, используют детекторы лжи, тотальный компьютерный контроль, кибернадзор за населением.

Кибернадзор применяется и в политической борьбе. «Уотер-гейт» ярко это продемонстрировал. Подобный инцидент произошел и в Канаде. В условиях низкой политической культуры населения информатизация на словах может представляться как средство демократизации, расширения свобод и т.п., а на деле использоваться для злоупотребления властью, негласного нарушения конституционных свобод, постепенной эволюции демократического государства в тоталитарное.

Четвертая группа информационных опасностей - использование новой информационной технологии в политических целях. Попытки внедрения информационного тоталитаризма (экспансионизма, колониализма) вполне объяснимы. Ведь рост воздействия средств массовой информации (СМИ) на ход и содержание политических процессов, функционирование механизма власти – одна из доминирующих тенденций современного общественного развития.

Борьба за контроль над новыми средствами массовой информации и информационной структурой, их использование для учета и обработки общественного мнения стали центральной проблемой во

внутриполитической жизни государств, особенно во время избирательных кампаний.

Таким образом, роль и значение информационной безопасности в обществе возрастают. Отставание в информатике может привести в перспективе к уязвимости компьютерных сетей страны и в целом всей ее информационной, управленческой инфраструктуры.

2. Основные составляющие информационной безопасности

Как было уже отмечено выше, ***информационная безопасность*** – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, комплексный подход (рис.2).

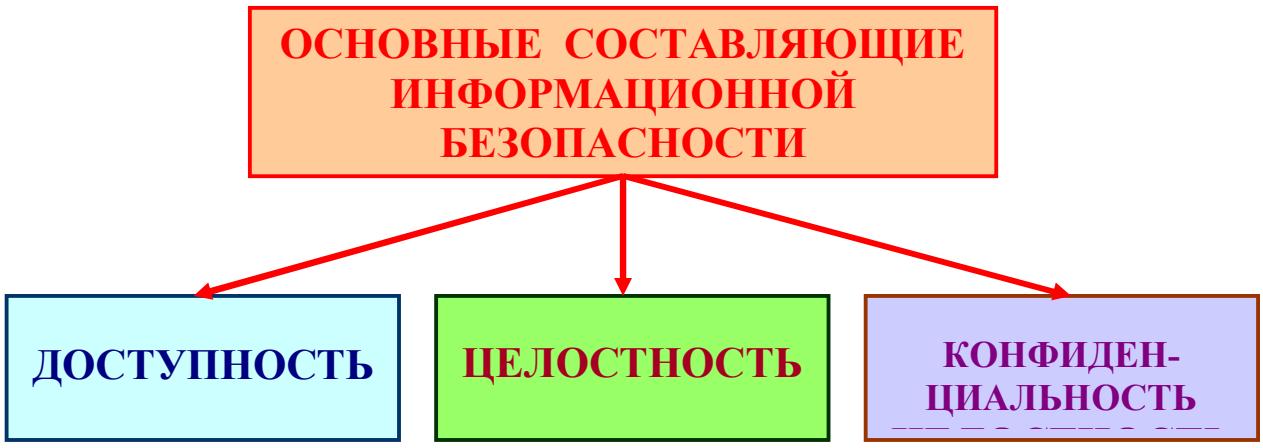

Рис. 2. Основные составляющие информационной безопасности

Как известно, спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение ***доступности***, ***целостности*** и ***конфиденциальности*** информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но это слишком специфический аспект и обычно специалисты в области информационной безопасности отдельно его не выделяют.

Доступность – возможность за приемлемое время получить требуемую информационную услугу.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем *субъектам информационных отношений*. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент *информационной безопасности*.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Под ***целостностью*** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики

комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

Наконец, ***конфиденциальность*** – это защита от несанкционированного доступа к информации.

Конфиденциальность – самый проработанный у нас в стране аспект *информационной безопасности*. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий *субъектов информационных отношений*, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Следует отметить, что конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

3. Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни

рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Если рассматривать ***безопасность*** в качестве общенаучной категории, то она может быть определена как некоторое состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой - ее функционирование не создает угроз для элементов самой системы и внешней среды. При таком определении мерой безопасности системы являются:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз - степень (уровень) сохранения системой своей структуры, технологи и эффективности функционирования при воздействии дестабилизирующих факторов;

- с точки зрения отсутствия угроз для элементов системы и внешней среды - степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам самой системы или внешней среде.

Чисто механическая интерпретация данных формулировок приводит к следующему определению информационной безопасности:

Информационная безопасность - такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Именно такое понятие информационной безопасности положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации. Приведенное определение представляется достаточно полным и вполне корректным. Однако, для того, чтобы служить более конкретным ориентиром в направлении поиска путей решения проблем информационной

безопасности, оно нуждается в уточнении и детализации его основополагающих понятий. При этом отправной точкой может служить тот факт, что информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима (т.е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой сама может быть источником большого числа разноплановых угроз как для элементов самой системы, так и для внешней среды. Отсюда естественным образом вытекает, что *обеспечение информационной безопасности* в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

1) защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;

2) защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;

3) защита внешней среды от информационных угроз со стороны рассматриваемой системы.

В соответствии с изложенным общая схема обеспечения информационной безопасности может быть представлена так, как показано на рис 3.

Естественно, что проблемы информационной безопасности являются производными относительно более общих проблем информатизации. Поэтому содержание проблем информационной безопасности должно формироваться в строгом соответствии с содержанием проблем информатизации, а концептуальные подходы к их решению должны взаимоувязываться с концепциями информатизации.

К основным концептуальным вопросам информатизации, на базе которых должны решаться и проблемы информационной безопасности, очевидно, могут быть отнесены:

- сущность информатизации;

- конечные результаты информатизации;

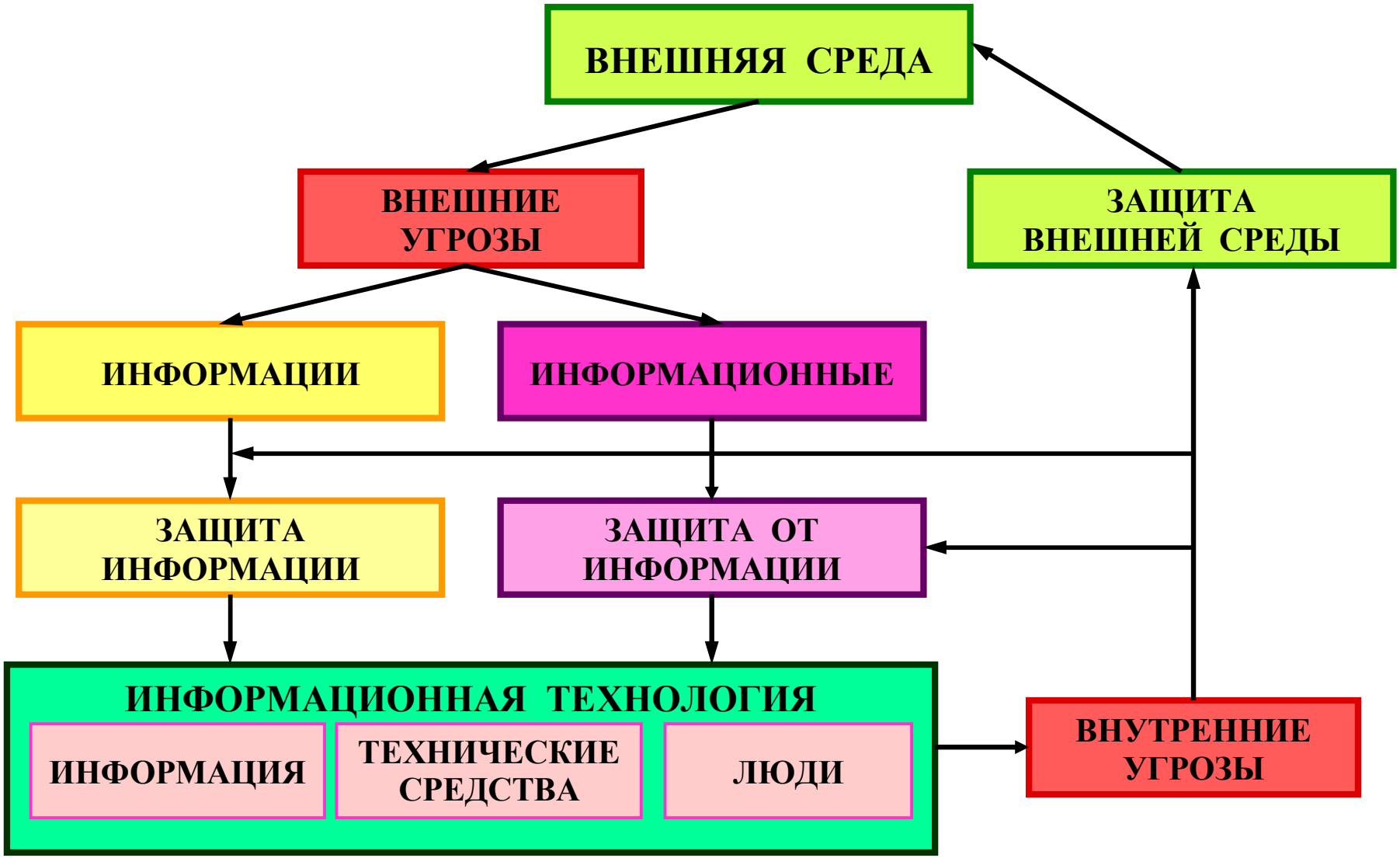

Рис. 3. Общая схема обеспечения информационной безопасности

- пути, средства и методы достижения основных результатов информатизации.

Не вдаваясь в философские аспекты информатизации, а взяв за основу ее прагматическое значение, можно с полным основанием утверждать, что сущность информатизации заключается в формировании такой информационной среды, в которой имелись бы все объективные предпосылки, необходимые для наиболее рационального информационного обеспечения всех сфер деятельности современного общества. Создание такой среды естественно предполагает всеобщую компьютеризацию, однако она представляет собой лишь компонент (хотя и один из важнейших) формирования общей инфраструктуры информационной среды.

В этих условиях производство, переработка и использование информации становятся важнейшей отраслью экономики, которая и получила общепризнанное название информационной индустрии. Таким образом, создание объективных предпосылок, необходимых для формирования информационной индустрии, и составляет основное содержание информатизации современного общества. При этом научно-методологическим базисом этого процесса служит такая отрасль науки, как информатика.

Перед информатикой фактически стоят две основные задачи: изучение информационных проблем общества и разработка путей, методов и средств наиболее рационального их решения. Изучение информационных проблем поставлено нами на первое место совсем не случайно. Этим однозначно определяется, что такое изучение является исходным базисом для реализации второй основной задачи информатики - разработки путей, методов и средств наиболее рационального решения этих проблем и, прежде всего удовлетворения информационных потребностей общества в процессе его жизнедеятельности.

Таким образом, пути, методы и средства информатизации должны разрабатываться исходя из информационных потребностей. Однако, в

соответствии с законом об обратной связи, и информационные потребности общества должны максимально приспосабливаться к возможностям их удовлетворения. Это означает, что информационные процессы в различных сферах деятельности должны быть целенаправленно подготовлены к переводу их на индустриальные методы осуществления.

Структурированные таким образом информационные потребности общества и являются одной из основных предпосылок для разработки необходимого арсенала методов и средств информатизации. Основу этого арсенала должны составлять унифицированные методы и современные средства обработки информации. На их базе и должна разрабатываться концепция индустриализации переработки информации и необходимые для этого информационные технологии.

Объективные предпосылки индустриализации процесса информационного обеспечения различных сторон деятельности современного общества создаются совокупностью результатов, полученных в последнее время в рамках информатики. К ним, прежде всего, относятся:

- системная классификация информации;
- унификация структуры информационного потока;
- унификация процедур (задач) обработки информации;
- систематизация методов обработки информации;
- унификация информационной технологии;
- формирование концепции управления процессами обработки информации по унифицированной технологии.

Последний из приведенных здесь результатов носит многоаспектный характер. Причем одной из основных его составляющих является проблема обеспечения информационной безопасности.

Резюмируя, сегодня можно выделить следующие наиболее острые проблемы развития теории и практики обеспечения информационной безопасности:

- создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);

- разработка научно обоснованных нормативно-методических документов по обеспечению информационной безопасности на базе исследования и классификации угроз информации и выработки стандартов требований к защите;

- стандартизация подходов к созданию систем защиты информации и рационализация схем и структур управления защитой на объектовом, региональном и государственном уровнях.

Решение спектра перечисленных задач имеет важное значение для реализации положений Доктрины информационной безопасности и Концепции национальной безопасности Российской Федерации.

4. Методология и логика информационной безопасности

4.1. Общее понимание информационной безопасности

Как было отмечено выше, понятие «информация» в современных условиях употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, по оценке специалистов, удваивается каждые три-пять лет. Такое положение приводит к заключению, что XXI век будет веком торжества теории и практики **ИНФОРМАЦИИ - *информационным веком***.

Информационное общество - концепция постиндустриального общества, новая историческая фаза развития цивилизации, в которой главными продуктами производства являются информация и знания.

Отличительными чертами информационного общества являются:

- увеличение роли информации и знаний в жизни общества;

- возрастание доли информационных коммуникаций, продуктов и услуг в валовом внутреннем продукте;

- создание глобального информационного пространства, обеспечивающего: а) эффективное информационное взаимодействие людей, б) их доступ к мировым информационным ресурсам и в) удовлетворение их потребностей в информационных продуктах и услугах.

Поэтому правомерно задать вопрос: так что же такое *информация*?

Информация (*information*) – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, которые уменьшают степень неопределенности и неполноту знаний.

В настоящее время общепринято считать, что информация – это мера порядка, который противостоит хаосу, что это мера сложности системы, характеристика внутреннего разнообразия системы, это мера вероятностного выбора одной из возможных траекторий развития того или иного процесса. Известно, что информация может иметь различную форму, включая данные, заложенные в компьютерах, письма или памятные записки, досье, формулы, чертежи, диаграммы, модели продукции и прототипы, диссертации, судебные документы и многое другое.

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения *потребителя*, качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения *обладателя* - сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

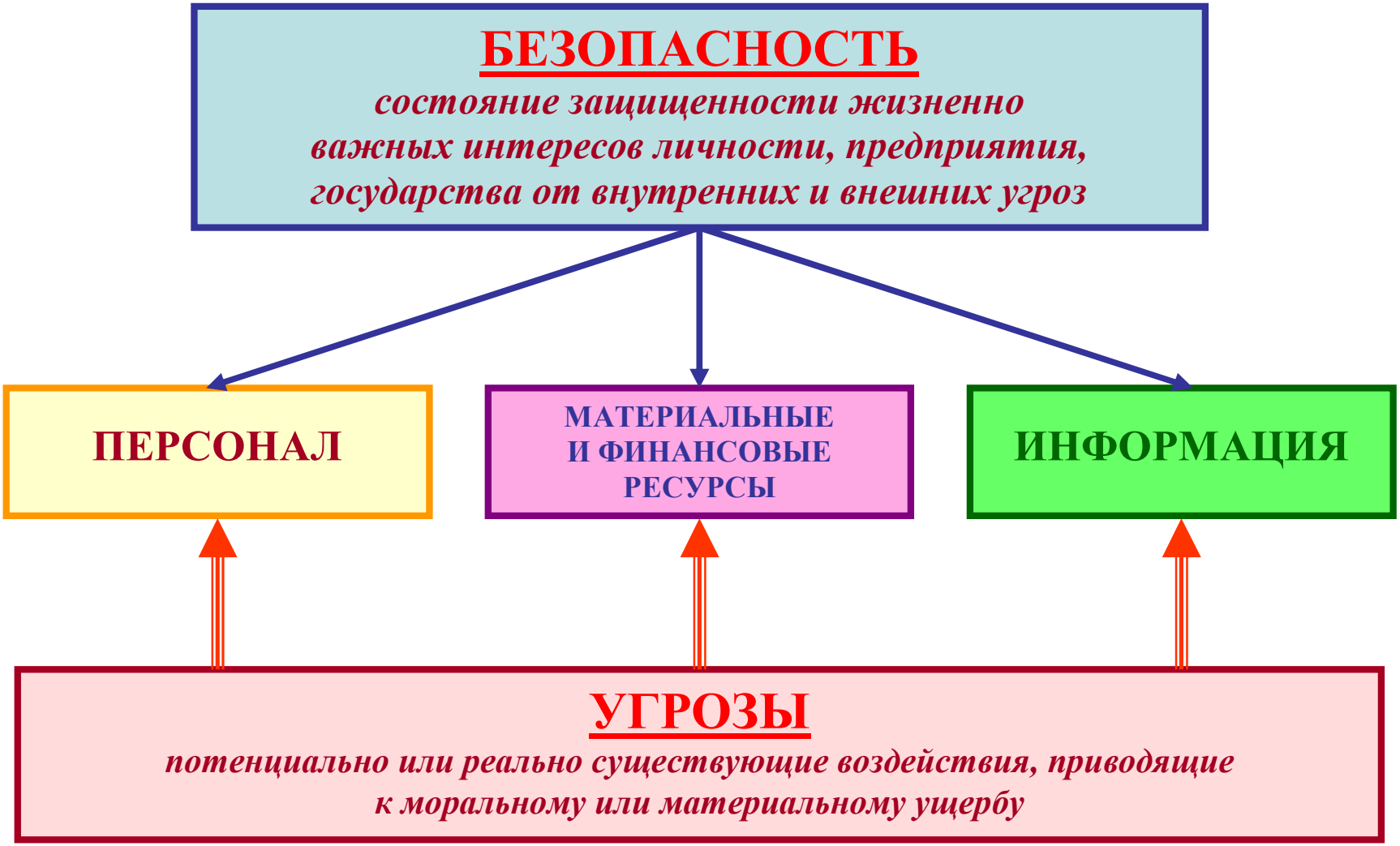

Рис. 4. Общее понимание безопасности

В целом, понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности такие, как *персонал*, *материальные и финансовые средства* и *информацию* (рис. 4).

Теория информационной безопасности, как одно из новых современных направлений, настоятельно нуждается в интенсивной разработке теоретико-методологического основания. В противном случае может быть нанесен интеллектуальный ущерб формированию информационного общества, а в итоге – к отставанию от современного процесса цивилизационной трансформации.

4.2. Теоретико-методологические основы информационной безопасности

Синтез категорий «теория» и «методология» дает теоретико-методологические основы любой отрасли знаний. Поэтому наиболее правильным будет говорить о методолого-теоретических основах, так как *методология* – по существу есть база для *теории*, а не наоборот.

Методология (от греч. *methodos* - способ познания, исследования явлений природы и общественной жизни и ***logos*** – слово, понятие, учение) – учение о научном методе познания; совокупность методов, применяемых в науке.

«Философский энциклопедический словарь» в свою очередь дает такое определение: методология – система принципов и способов организации и построения теоретической и практической деятельности, а также учение об этой системе.

Методология – тип рационально-рефлексивного сознания, направленный на изучение, совершенствование и конструирование методов. Она включает в себя методологические представления и концепции различного уровня и широты охвата (общенаучная, философская

методология, методология междисциплинарного уровня, методология частных наук. В настоящее время активно разрабатываются методологические концепции, связанные с отдельными видами деятельности.

Методология познания и преобразования человеком современного мира развивается широким фронтом на различных уровнях знания и в различных его областях и приобретает в последнее время все большее значение в общем комплексе научных исследований. Являясь учением о методах и теориях, методология дает характеристику компонентов научного исследования, отражает совокупность исследовательских средств и формирует представление о последовательности проведения исследования.

В настоящее время имеется ряд различных и уже принятых определений и трактовок методологии, которые отличаются от формулировки, приведенной выше. Однако все принятые трактовки методологии имеют определенные основания. Более того, можно обнаружить пересечения и связь между ними, но наиболее типичными характеристиками методологии все же являются (рис. 5):

- методология – есть совокупность приемов исследования, методов, применяемых в какой-либо науке;

- методология – это применение принципов мировоззрения к процессу познания, к духовному творчеству вообще и к практике;

- методология – это учение о методах, особо научное направление, связанное с изучением познавательных средств.

Таким образом, методология может определяться как система наиболее общих принципов, положений и методов, составляющих основу той или иной науки. Поэтому с учетом выше сказанного совокупность идей, принципов, положений и методов в информационной сфере, а также теоретическое обоснование этих идей, принципов, положений и методов составляют суть ***методологии информационной безопасности***.

Рис. 5. Типичные характеристиками методологии

Другими словами, *методология информационной безопасности* представляет собой научную методологию и логику научных исследований информационной сферы общества (информационного общества), направленную на обеспечение информационной безопасности государства как составной части национальной безопасности.

С другой стороны, ***теория*** (от греч. *theoría*, что означает рассматриваю, исследую) *в широком смысле* – это комплекс взглядов, представлений, идей, направленных на истолкование и объяснение какого либо явления; *в узком смысле* - это высшая, самая развитая форма организации научного знания, дающая целостное представление о закономерностях и существенных связях определенной области деятельности – объекта данной теории. Ее формы – законы науки, классификации, типологии, первичные объяснительные схемы.

Другими словами любая теория представляет собой форму достоверных научных знаний: представляющая собой множество логически увязанных между собой допущений и суждений; дающая целостное представление о закономерностях и существенных характеристиках объектов и основывающаяся на окружающей реальности.

С учетом выше сказанного ***теория информационной безопасности*** представляет собой высшую форму научного знания, дающую целостное представление о закономерностях и существующих связях в информационной сфере и определяющую цели, задачи, принципы и основные направления по обеспечению информационной безопасности.

Таким образом, если методология информационной безопасности включает в себя обоснование законов, разработку методов, принципов исследования на концептуальном, парадигмальном уровне, то теория информационной безопасности, применяя данный научный арсенал и прилагая его непосредственно к объекту ИБ, к определенным явлениям, процессам, видам деятельности и отношений, дает систему научных взглядов, представлений, идей, а главное – открывает и описывает законы,

Рис. 6. Сущность синтеза методологии и теории информационной безопасности

дает классификацию, типологию, объяснительные схемы исследуемого объекта и формирует предмет информационной безопасности как науки. В этом заключается синтез методологии и теории, а, следовательно, онтологии «теоретико-методологических» основ информационной безопасности (рис. 6).

4.3. Междисциплинарный подход исследования информационной безопасности

Методология информационной безопасности должна решать в первую очередь проблемы, обусловленные развитием информационных технологий, и базироваться, на наш взгляд на использовании ***междисциплинарного подхода***, который в современных условиях является наиболее перспективным и продвинутым методом исследования сложных самоорганизующихся систем.

Междисциплинарный подход – метод получения знаний и их последующей интеграции на стыке между двумя и более научными дисциплинами.

Однако междисциплинарный подход в научном познании вовсе не сводится к тому, чтобы совместно рассматривать проблемы из разных областей науки. Любое междисциплинарное исследование должно отвечать прежде всего следующему необходимому условию: *поставленная научная проблема может быть совместно рассмотрена с различных позиций, принадлежащим разным, иногда далеко отстоящим друг от друга, наукам, которые в свою очередь могут характеризоваться разными формами и средствами проведения научных исследований*. Это основное и необходимое, но не достаточное условие междисциплинарного подхода.

При междисциплинарном подходе в каждой конкретной предметной области совместное и взаимосвязанное рассмотрение научных проблем должно базироваться на реальных основаниях структурного характера, то

есть должны присутствовать такие объективные структурные связи по своей природе, в силу которых образуются пограничные и комплексные объекты, представляющие собой предмет исследования для различных фундаментальных наук и научных дисциплин.

Междисциплинарный подход в современной науке, понимаемый в самым широком смысле, охватывает разные формы проведения пограничных и комплексных исследований с формированием соответствующего типа научных теорий и течений. Все они имеют специфические и объективные основания, а тем самым и специфическое значение, для развития научного познания.

Необходимо отметить, что различные формы проведения пограничных и комплексных исследований по сути своей не являются равноправными – между ними присутствуют определенные отношения субординаций:

- во-первых, некоторые междисциплинарные исследования обычно являются предварительными для более высокой стадии применения междисциплинарного подхода, связанного с формированием и дальнейшим развитием соответствующего типа научной теории или даже научной области;

- во-вторых, проведение исследований и формирование научных теорий и даже научных областей на стыке двух или более наук приводит к формированию новых комплексных (междисциплинарных) наук.

Формирование комплексных наук, какой является информационная безопасность в современных условиях, – вершина проявления междисциплинарного подхода в современной науке. Исходя из этого можно заключить, что междисциплинарный подход представляет собой высшую форму интегративной тенденции в науке, которая характеризуется возникновением комплексных наук, объединяющих научные проблемы из разных наук и научных дисциплин, создавая тем самым новый тип границ в пространстве научных проблем. Поэтому из-за недостаточности традиционных подходов в современной науке формируется новая методология

научных исследований, важное место в которой занимают три фундаментальных и взаимно дополняющих друг друга подхода к научному познанию: системный, синергетический и информационный (рис. 7).

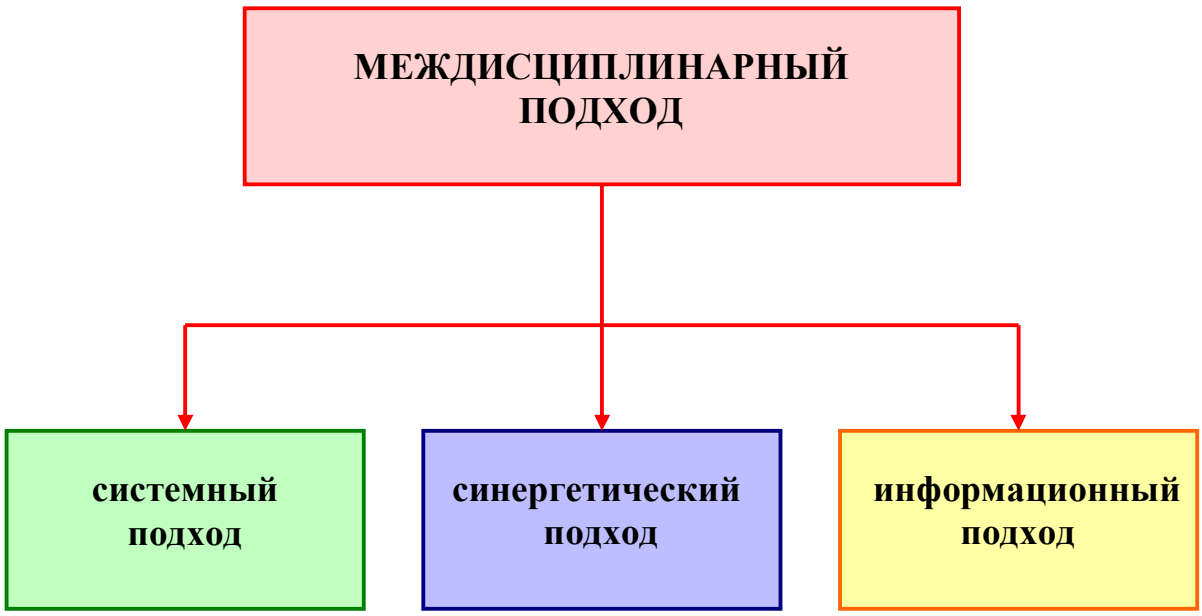

Рис. 7. Схема междисциплинарного подхода в современной науке

Комплексное использование системного, синергетического и информационного подходов является ярким проявлением эффективного применения междисциплинарного подхода и базируется на основном тезисе, что случайность и закономерность в определенной степени взаимосвязаны. Поэтому комплексное использование системного, синергетического и информационного подходов в современной науке с философской точки зрения не что иное, как выражение и развитие общих законов диалектики: о переходе количественных изменений в качественные, единства и борьбы противоположностей, отрицание отрицания, которые конкретно для информационной безопасности отражают универсальные формы, пути и движущую силу ее развития и познания.

В своем происхождении и историческом развитии информационная безопасность представляет собой логическое выражение объективной

диалектики мира и его познания в динамике развития информационных технологий. Однако научные исследования в информационной сфере без использования исторического подхода к научному познанию развития информационных систем и современных информационных технологий будут неполными.

С другой стороны, сильное влияние человеческого фактора в информационной сфере приводит к необходимости использования системно-деятельностного подхода, как эффективного метода исследования информационной безопасности и ее обеспечения в современных условиях. Поэтому проблема информационной безопасности должна исследоваться именно с таких основополагающих позиций, как комплексное применение системного, системно-деятельностного, синергетического, собственно информационного и исторического подходов (рис. 8).

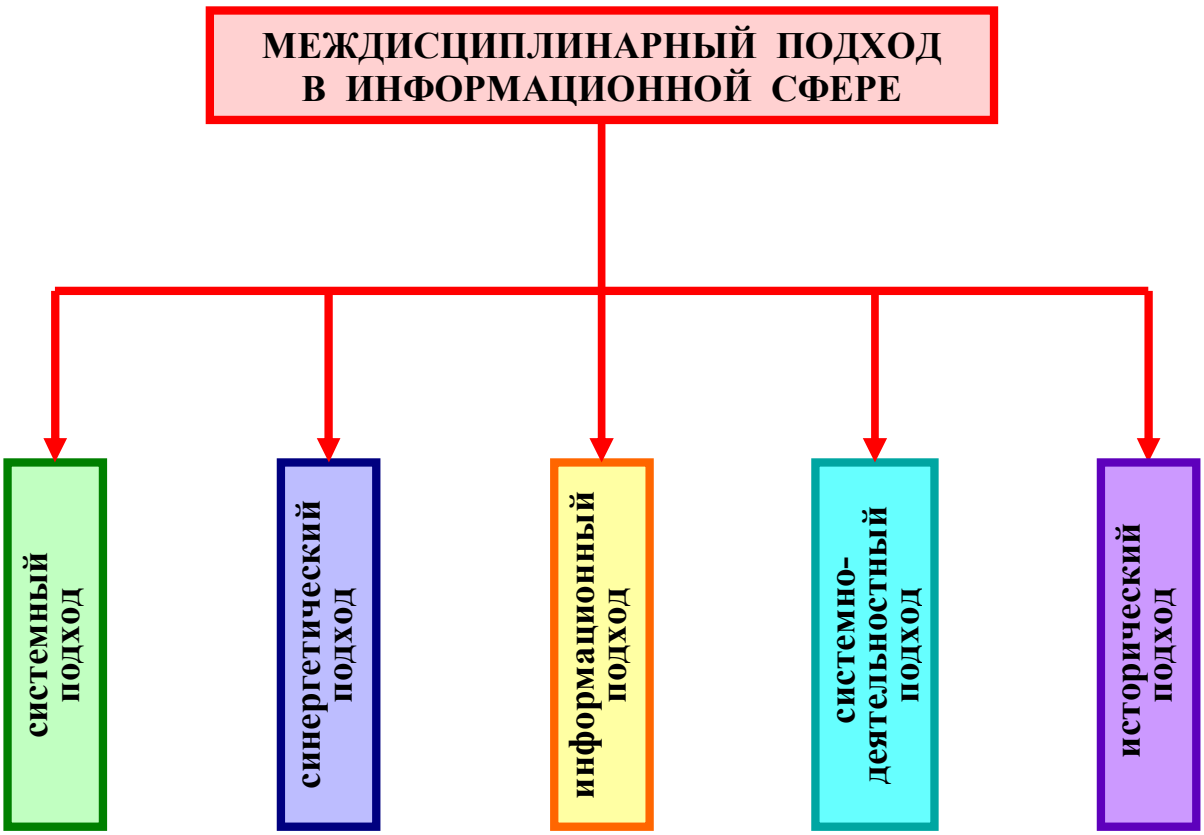

Рис. 8. Схема междисциплинарного подхода в информационной сфере

Таким образом, совокупность методологических подходов и методов научных исследований информационной безопасности представляют собой определенную многоуровневую систему, которая имеет как внутренние, так и внешние связи с методологией других наук и научных дисциплин, которая позволяет исследовать информационную безопасность именно с позиций комплексного подхода (рис. 9).

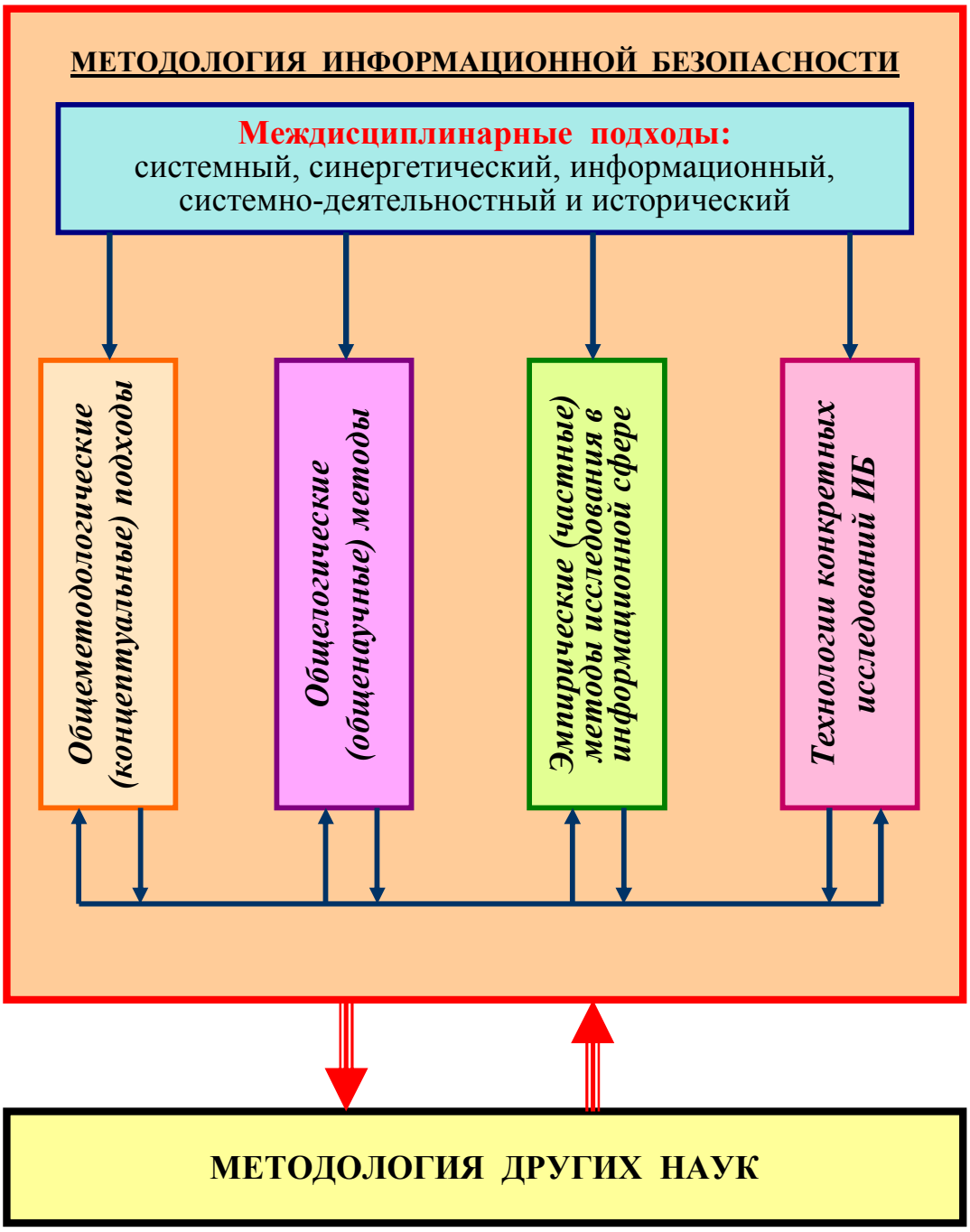

Рис.9. Сущность методологии информационной безопасности

Заключение

Информационная безопасность в начале третьего тысячелетия уверенно выходит на первое место в системе национальной безопасности. Поэтому наиболее актуальным сейчас является афоризм «кто владеет информацией, тот владеет миром». Информация превратилась из абстрактного понятия в едва ли не самый ценный объект во Вселенной и ход всех значимых событий в науке, коммерции, социуме связан с процессами производства и владения информацией. С другой стороны, информационная безопасность - это сравнительно молодая, быстро развивающаяся область информационных технологий, для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями информационных технологий базис – концептуальные основы информационной безопасности. Поэтому совокупность методологических подходов и методов научных исследований информационной безопасности должна представлять собой определенную многоуровневую систему, которая имела бы как внутренние, так и внешние связи с методологией других наук и научных дисциплин и которая позволила бы исследовать информационную безопасность с позиций комплексного, междисциплинарного подхода на базе совокупности системного, синергетического, информационного, системно-деятельностного и исторического подходов.

Литература

1. Батурин Ю.М. Космическая дипломатия и международное право. – Звездный городок, 2006. – 138 с.
2. Блауберг И.В., Юдин Э.Г. Становление и сущность системного подхода. – М., 1973.
3. Галатенко В.А. Основы информационной безопасности. Курс лекций. Учебное пособие / Под ред. В.Б. Бетелина. – М.: ИНТУИТ, 2004. – 264 с.
4. Жук Е.И. Пилотируемая космонавтика в интересах национальной и коллективной безопасности (политический аспект). – Звездный городок, 2003. – 406 с.
5. Жук Е.И. Пилотируемая космонавтика: международная и национальная безопасность. – Звездный городок, 2008. – 446 с.
6. Золотарев В.А. Военная безопасность Государства Российского. – М.: Кучково поле, 2001. – 484 с.
7. Золотарев В.А. Военная безопасность Отечества (историко-правовое исследование). – 2-е изд. – М.: «КАНОН-пресс»-«Кучково поле», 1998. – 462 с.
8. Климович А.Т. Национально-государственная безопасность России. Учебное пособие. – М.: ВАГШ, 1996.
9. Леонтьев А.Н. Деятельность. Сознание, Личность. – М.: Политиздат, 1977. – 304 с.
10. Лисовой В.М. Основы военной доктрины государства. Учебное пособие. – М.ВАГШ, 2000. – 58 с.
11. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.
12. Манилов В.Л. Безопасность в эпоху партнерства. – М.: ТЕРРА, 1999. – 368 с.

13. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность: Учеб. пособие для сред. профессионального образования / Под ред. С.А. Клейменова. – М.: Издательский центр «Академия», 2005 – 336 с.

14. Национальная безопасность: актуальные проблемы. Курс лекций / Отв. ред. Шаваев А.Х. – М.: ВАГШ, 1999. – 420 с.

15. Национальная политика России: история и современность. – М.: «Русский мир», 1997. – 680 с.

16. Общая теория национальной безопасности: Учебник / Под. общ. ред. А.А. Прохожева. – М.: РАГС, 2002. – 320 с.

17. Основы информационной безопасности: Учебное пособие / О.А.Акулов, Д.Н.Баданин, Е.И.Жук и др. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2008. – 161 с.

18. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие для студентов учреждений среднего профессионального образования. – М.: ФОРУМ: ИНФА-М, 2005 – 368 с.

19. Прангишвили И.В. Системный подход и общесистемные закономерности. – М.: СИНТЕГ, 2000. – 528 с.

20. Пригожин И., Стенгерс И. Порядок из хаоса. Новый диалог человека с природой: Пер. с анг. – М.: Едиториал УРСС, 2003. – 312 с.

21. Российский энциклопедический словарь: В 2 кн./Гл. ред. А.М.Прохоров. – М.: Большая российская энциклопедия, 2001. – Кн. 1 : А-Н. – С. 1023 кн. 2: Н-Я. – 2015 с.

22. Садовский В.Н. Основание общей теории систем. Логико-методологический анализ. – М., 1974.

23. Семененко В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2004 – 215 с.

24. Советский энциклопедический словарь / Гл. ред. А.М. Прохоров. – 2-е изд. – М.: Сов. энциклопедия, 1983. – 1600 с.

25. Стратегия национальной безопасности США в следующем столетии (перевод). – М., 1998. – 86 с.

26. Философский словарь / Под ред. И.Т. Фролова. – 5-е изд., перераб. и доп. – М.: Политиздат, 1991. – 560 с.

27. Философский энциклопедический словарь. – М.: ИНФА-М, 2000. – 576 с.

28. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – 3-е изд. – М.: Академический Проект: Трикста, 2005 – 544 с.