Современные угрозы информационной безопасности в России

Угрозы ИБ

- Согласно Закону о безопасности под **угрозой безопасности понимается *совокуп-***
- ***ность условий и факторов, создающих опасность жизненно важным интересам личности,***
- ***общества и государства. Концепция национальной безопасности РФ не дает определения***
- угрозы, но называет некоторые из них в информационной сфере. Так, опасность представ-
- ляют:
- – стремление ряда стран к доминированию в мировом информационном пространстве;
- – вытеснение государства с внутреннего и внешнего информационного рынка;
- – разработка рядом государств концепции информационных войн;
- – нарушение нормального функционирования информационных систем;
- – нарушение сохранности информационных ресурсов, получение несанкционирован-
- ного доступа к ним.
- Это так называемые ***внешние угрозы, которые обусловлены конкурентным харак-***
- ***тером развития межгосударственных и международных отношений. Соответственно***
- существуют и ***внутренние угрозы, связанные во многом с недостаточным проведением***
- ***экономических, социально-политических и иных преобразований в сфере ИБ.***

Угрозы ИБ

- Концепция
- национальной безопасности называет их в качестве предпосылок возникновения угроз. С
- учетом этих предпосылок, по нашему мнению, к источникам внутренних угроз можно отне-
- сти:
- – отставание России в сфере информатизации органов государственной власти;
- – несовершенство системы организации государственной власти по формированию и
- реализации единой государственной политики обеспечения ИБ;
- – криминализацию общественных отношений, рост организованной преступности;
- – увеличение масштабов терроризма;
- – обострение межнациональных и осложнение внешних отношений.
- Для нейтрализации информационных угроз существует исторически сложившаяся
- система сохранения государственной тайны, включающая подсистемы:
- – криптографической сети конфиденциальной связи;
- – противодействия иностранным техническим разведкам;
- – обеспечения режима секретности на закрытых государственных объектах.
- Наряду с традиционными приоритетами иностранных технических разведок в сферу
- их интересов все в большей мере вовлекаются вопросы технологий, финансов, торговли,
- ресурсов, доступ к которым открывается в связи с конверсией, развитием международных
- интеграционных процессов, широким внедрением компьютерных технологий. Из существу-
- ющих информационных угроз наиболее актуальными являются угрозы экономической без-
- опасности предприятий и фирм, определяемые недобросовестной конкуренцией, экономи-
- ческим и промышленным шпионажем. Промышленный шпионаж существовал всегда.

Угрозы ИБ

- **Промышленный шпионаж представляет собой *несанкционированную передачу кон-***
- *фиденциальной технологии, материалов, продукции, информации о них.*
- ***Методы и способы ведения шпионажа остаются неизменными на протяжении многих***
- столетий развития общества и государства. При этом меняются только средства и формы его
- ведения. К таким методам относятся: подкуп, шантаж, деятельность послов-шпионов, пере-
- хват сообщений, представленных на различных носителях (магнитные носители, письма и
- др.).
- А. В. Артемов. «Информационная безопасность. Курс лекций»
- 12
- Что касается ***анализа полученной информации, то все осталось без изменений. Им***
- занимается человек или группа людей, осуществляющих аналитико-синтетическую перера-
- ботку информации, в том числе с использованием новых информационных технологий.
- Развитие техники вплоть до начала XX в. не влияло на средства несанкционирован-
- ного получения информации: сверлили дырки в стенах и потолках, использовали потайные
- ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появле-

Угрозы ИБ

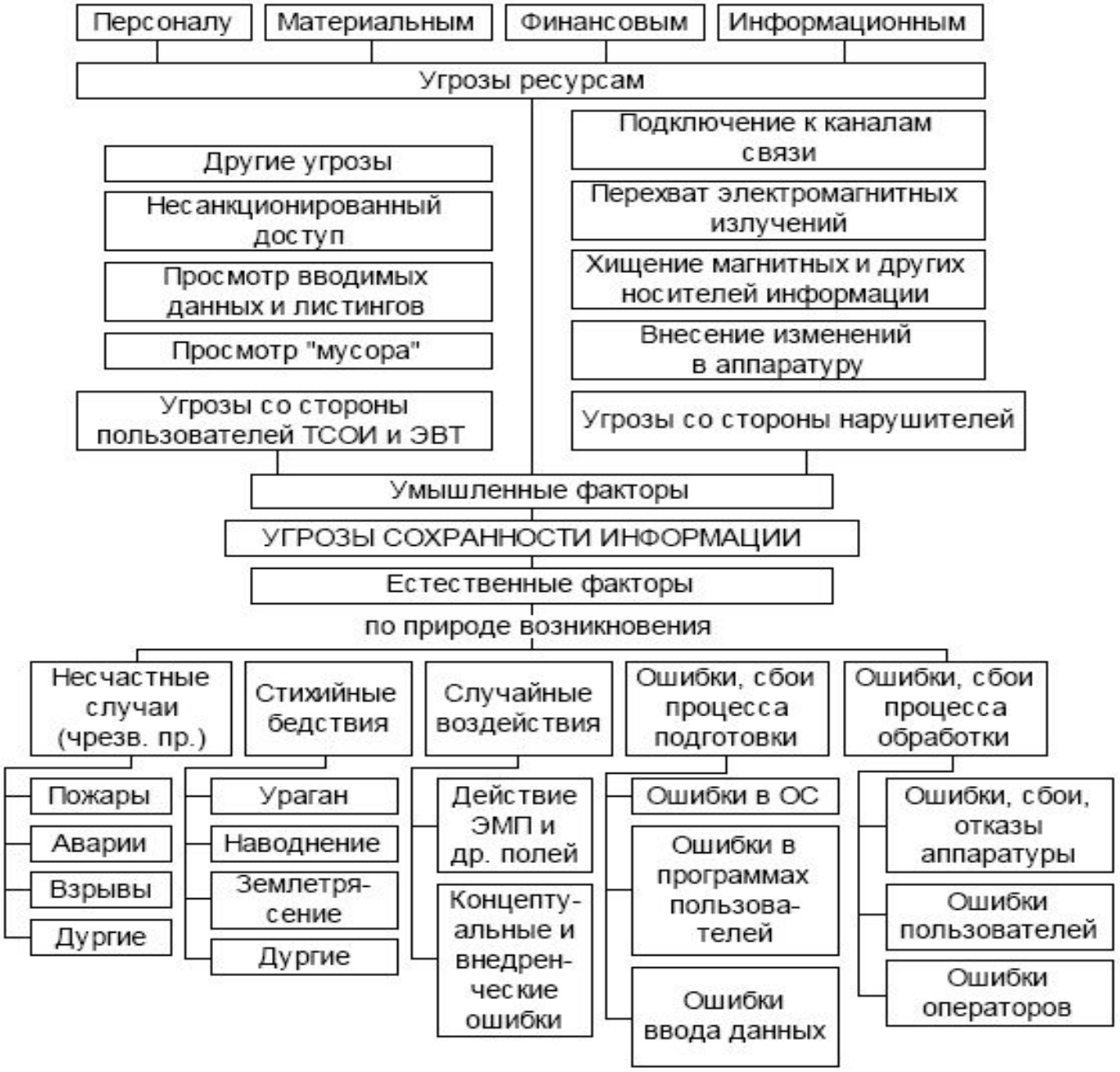
Анализ результатов исследований угроз информации позволяет утверждать, что одной из основных угроз государственной безопасности Российской Федерации являются попытки западных спецслужб добывать ***конфиденциальные сведения, составляющие государственную***, промышленную, банковскую и другие виды тайн. Ведущие западные страны продолжают модернизировать и развивать свои разведывательные службы, совершенствовать техническую разведку, наращивать ее возможности.

С учетом рассмотренного содержания понятия угрозы государству, обществу и личности в широком смысле рассмотрим угрозы, непосредственно воздействующие на обрабатываемую конфиденциальную информацию. Система угроз безопасности представляет собой реальные или потенциально возможные действия или условия, приводящие к хищению, искажению, несанкционированному доступу, копированию, модификации, изменению, уничтожению конфиденциальной информации и сведений о самой системе и, соответственно, к прямым материальным убыткам.

При этом угрозы сохранности информации определяются случайными и преднамеренными разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренного корыстного воздействия несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, модификации и использование обрабатываемой информации. Анализ содержания свойств угроз позволяет предложить следующие варианты их классификации (рис. 1).

Угрозы ИБ

- Проявление угроз характеризуется рядом закономерностей. Во-первых, незаконным
- овладением конфиденциальной информацией, ее копированием, модификацией, уничтоже-
- нием в интересах злоумышленников, с целью нанесения ущерба. Кроме этого, непреднаме-
- ренные действия обслуживающего персонала и пользователей также приводят к нанесению
- определенного ущерба. Во-вторых, основными путями реализации угроз информации и без-
- опасности информации выступают:
- – агентурные источники в органах управления и защиты информации;
- – вербовка должностных лиц органов управления, организаций, предприятий и т. д.;
- – перехват и несанкционированный доступ к информации с использованием техниче-
- ских средств разведки;
- – использование преднамеренного программно-математического воздействия;
- – подслушивание конфиденциальных переговоров в служебных помещениях, транс-
- порте и других местах их ведения.


Персоналу
Материальным
Финансовым
Информационным
Угрозы ресурсам
Подключение к каналам связи
Другие угрозы
Несанкционированный доступ
Перехват электромагнитных излучений
Просмотр вводимых данных и листингов
Хищение магнитных и других носителей информации
Просмотр "мусора"
Внесение изменений в аппаратуру
Угрозы со стороны пользователей ТСОИ и ЭВТ
Угрозы со стороны нарушителей
Умышленные факторы
УГРОЗЫ СОХРАННОСТИ ИНФОРМАЦИИ
Естественные факторы
по природе возникновения
Несчастные случаи (чрезв. пр.)
Стихийные бедствия
Случайные воздействия
Ошибки, сбои процесса подготовки
Ошибки, сбои процесса обработки
Пожары
Аварии
Взрывы
Дургие
Ураган
Наводнение
Землетря-сение
Дургие
Действие ЭМП и др. полей
Концепту-альные и внедрен-ческие ошибки
Ошибки в ОС
Ошибки в программах пользова-телей
Ошибки ввода данных
Ошибки, сбои, отказы аппаратуры
Ошибки пользователей
Ошибки операторов

Угрозы ИБ

- Основными факторами воздействия угроз, обусловливающими информационные
- потери и приводящими к различным видам ущерба, возрастание убытков от неправомерных
- действий, являются:
- – несчастные случаи, вызывающие выход из строя оборудования и информационных
- ресурсов (пожары, взрывы, аварии, удары, столкновения, падения, воздействия химических
- или физических сред);
- – поломки элементов средств обработки информации;
- – последствия природных явлений (наводнения, бури, молнии, землетрясения и др.);
- – кражи, преднамеренная порча материальных средств;
- – аварии и выход из строя аппаратуры, программного обеспечения, баз данных;
- – ошибки накопления, хранения, передачи, использования информации;
- – ошибки восприятия, чтения, интерпретации содержания информации, соблюдения
- правил, ошибки как результат неумения, оплошности, наличие помех, сбоев и искажений
- отдельных элементов и знаков или сообщения;

Угрозы ИБ

- – ошибки эксплуатации: нарушение защиты, переполнение файлов, ошибки языка
- управления данными, ошибки при подготовке и вводе информации, ошибки операционной
- системы, программирования, аппаратные ошибки, ошибки толкования инструкций, пропуск
- операций и др.;
- – концептуальные ошибки внедрения;
- – злонамеренные действия в материальной сфере;
- – болтливость, разглашение; – убытки социального характера (уход, увольнение, заба-
- стовка и др.).
- Информационный ущерб в ряде случаев может быть оценен в зависимости от вида
- потерь. Это могут быть:
- *– потери, связанные с компенсацией или возмещением утраченных, похищенных мате-*
- *риальных средств, которые включают:*
- • стоимость компенсации возмещения другого косвенно утраченного имущества;
- • стоимость ремонтно-восстановительных работ;
- • расходы на анализ и исследование причин и величины ущерба;
- • другие расходы;

Угрозы ИБ

- *– дополнительные расходы на персонал, обслуживающий технические средства обра-*
- ботки конфиденциальной информации, восстановление информации, возобновление работы
- информационных систем по сбору, хранению, обработке, контролю данных, в том числе рас-
- ходы:
- • на поддержку информационных ресурсов ТСОИ;
- • обслуживающий персонал, не связанный с обработкой информации;
- • специальные премии, расходы на перевозку и др.;
- *– эксплуатационные потери, связанные с ущербом банковских интересов или финан-*
- совыми издержками, потерей клиентов, заказчиков, требующие дополнительных расходов
- на восстановление: банковского доверия; размеров прибыли; утерянной клиентуры; доходов
- организации и др.;
- • утрата фондов или порча имущества, не подлежащего восстановлению, которые сни-
- жают финансовые возможности (деньги, ценные бумаги, денежные переводы и др.);
- • расходы и потери, связанные с возмещением морального ущерба, обучением, экспер-
- тизой и др.

Угрозы ИБ

- **Разглашение информации – это *умышленные или неосторожные действия долж-***
- *ностных лиц и граждан, которым в установленном порядке были доверены соответству-*
- *ющие сведения по работе, приведшие к оглашению охраняемых сведений, а также передача*
- *таких сведений по открытым техническим каналам. Разглашение выражается в сообще-*
- нии, передаче, предоставлении, пересылке, опубликовании, при обсуждении, утере и огла-
- шении любыми иными способами конфиденциальной информации лицам и организациям,
- не имеющим права доступа к охраняемым секретам. Разглашение информации может про-
- исходить по многим каналам, в том числе через почтовые отправления, радио, телевидение,
- печать и т. п. Разглашение возможно в ходе деловых встреч, бесед, при обсуждении совмест-
- ных работ, в договорах, в письмах и документах, деловых встречах и др. В ходе таких меро-
- приятий партнеры ведут интенсивный обмен информацией. Именно при общении между
- ними устанавливаются "доверительные" отношения, приводящие к оглашению коммерче-
- ских секретов.

Угрозы ИБ

- **Утечку информации в общем виде можно рассматривать как *бесконтрольный и***
- *неправомерный выход конфиденциальной информации за пределы организации или круга лиц,*
- *которым эта информация была доверена. При этом природа утечки охраняемой информа-*
- ции характеризуется как обстоятельствами происхождения, так и причинами, условиями
- возникновения утечки.
- Неправомерному овладению конфиденциальной информацией вследствие ***неудовле-***
- ***творительного управления персоналом со стороны должностных лиц, организаций и***
- ведомств способствует наличие следующих обстоятельств:
- – склонность сотрудников организации к излишней разговорчивости – 32 %;
- А. В. Артемов. «Информационная безопасность. Курс лекций»
- 16
- – стремление сотрудников зарабатывать деньги любыми способами и любой ценой –
- 24 %;
- – отсутствие в фирме службы безопасности – 14 %; – привычка сотрудников делится
- друг с другом информацией о своей служебной деятельности – 12 %;
- – бесконтрольное использование в фирме информационных систем – 10 %;
- – предпосылки возникновения конфликтных ситуаций в коллективе вследствие отсут-
- ствия психологической совместимости сотрудников, случайного подбора кадров, отсутствия
- работы руководителя по сплочению коллектива и др. – 8 %.

Угрозы ИБ

- Способы **несанкционированного доступа (НСД) как проблему утечки конфиденци-**
- альной информации предлагается рассматривать со следующих позиций. Вопрос обеспе-
- чения защиты от НСД связан с проблемой сохранности не только информации как вида
- интеллектуальной собственности, но физических и юридических лиц, их имущественной
- собственности и личной безопасности. Известно, что такая деятельность тесно связана с
- получением, накоплением, хранением, обработкой и использованием разнообразных инфор-
- мационных потоков. Как только информация представляет определенную цену, факт ее
- получения злоумышленником приносит ему определенный доход, ослабляя тем самым воз-
- можности конкурента. Отсюда главная цель противоправных действий – получение инфор-
- мации о составе, состоянии и деятельности объекта конфиденциальной информации для
- удовлетворения своих информационных потребностей в корыстных целях и внесение изме-
- нений в состав информации. Такое действие может привести к дезинформации в определен-
- ных сферах деятельности и отражаться, в частности, на учетных данных, результатах реше-

Угрозы ИБ

- ***Характерные нарушения при посещении предприятий командированными***
- ***лицами:***
- – допуск командированных лиц с ведома руководителей подразделений к конфиденци-
- альным работам и документам без соответствующего оформления разрешения;
- – невыполнение требований инструкций для внутренних объектов по сопровождению
- прибывших в подразделения командированных лиц;
- – отсутствие в предписаниях отметок о действительно выданной информации пред-
- ставителям других предприятий;
- – прием командированных лиц с предписаниями, в которых отсутствуют основания
- командирования (номер и дата хозяйственного договора, ТЗ совместного плана НИОКР и
- др.);
- – не определена степень конфиденциальности материалов, к которым допускается
- командированное лицо.

Угрозы ИБ

- ***Нарушения, связанные с проведением служебных совещаний:***
- – проведение совещаний без соответствующего разрешения руководителя предприя-
- тия или его заместителей;
- – допуск на совещание лиц, не имеющих отношения к обсуждаемым вопросам и уча-
- стие которых не вызывается служебной необходимостью;
- – несоблюдение очередности рассмотрения вопросов конфиденциального характера;
- А. В. Артемов. «Информационная безопасность. Курс лекций»
- 20
- – несоблюдение требований режима внутреннего объекта при проведении совещаний;
- – фотографирование, демонстрация конфиденциальных изделий, фильмов без согла-
- сования с СБ;
- – звукозапись выступлений участников совещания на носителе, не учтенном в СБ;
- – направление тетрадей (записей) секретного характера в учреждения, которых эти све-
- дения непосредственно не касаются;
- – недостаточное знание работниками, участвующими в приеме командированных лиц,
- требований инструкции о порядке приема командированных лиц (об этом заявили около
- 45 % опрошенных лиц).

Угрозы ИБ

- ***Нарушения при ведении конфиденциальных работ в рабочих помещениях заключа-***
- ются в отсутствии обеспечения:
- – специальных средств защиты конфиденциальной информации, связи, звукозаписи,
- звукоусиления, переговорных и телевизионных устройств;
- – средств изготовления и размножения документов;
- – средств пожарной и охранной сигнализации;
- – систем электронной часофикации, электрооборудования и других дополнительных
- технических средств защиты, исключающих утечку информации за счет побочных электро-
- магнитных излучений и наводок.
- Такие каналы утечки, как ***доступ и обращение с конфиденциальной информацией,***
- образуются за счет расширения круга лиц, имеющих допуск к документам, изделиям, тех-
- ническим заданиям.

Угрозы ИБ

- ***Нарушения в организации пропускного и внутриобъектового режима включают:***
- – утрату удостоверений, пропусков, ключей от режимных помещений, хранилищ, сей-
- фов (шкафов), личных печатей – 12 %;
- – пронос без разрешения СБ на территорию предприятия кино– и фотоаппаратуры,
- радиопередающей и принимающей, а также множительно-копировальной аппаратуры лич-
- ного пользования;
- – вынос из предприятия секретных документов и изделий без разрешения;
- – оставление незакрытыми и не опечатанными после работы помещений (хранилищ).
- Каналы утечки конфиденциальных сведений за счет ***неправильной организации про-***
- ***хождения технологической и преддипломной практики студентов проявляются в сле-***
- дующем: студенты и учащиеся вузов и средних специальных учебных заведений после про-
- хождения практики не зачисляются на постоянную работу, где они проходили практику и
- познакомились со сведениями, составляющими государственную или коммерческую тайну,
- и другие причины.

Угрозы ИБ

- ***Характерные нарушения при решении задач отраслевого и межотраслевого харак-***
- ***тера:***
- – включение конфиденциальных сведений в открытые документы с целью упрощения
- порядка доставки и согласования документов;
- – ведение секретных записей в личных блокнотах, записных книжках;
- – ознакомление с конфиденциальными работами и сведениями лиц, в круг служебных
- обязанностей которых они не входят;
- – направление адресатам конфиденциальных документов, к которым они не имеют
- отношения.
- Таким образом, проведенный анализ угроз информации позволяет уточнить ее свой-
- ства, подлежащие правовой защите. При этом содержание этих свойств будет рассматри-
- ваться с учетом положений действующих нормативных актов.