Методы и приемы обеспечения информационной безопасности

Под безопасностью информации (Information security) или **информационной безопасностью** понимают защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей её структуре.

- При рассмотрении проблем, связанных с обеспечением безопасности, используют понятие **«несанкционированный доступ»** – это неправомочное обращение к информационным ресурсам с целью их использования (чтения, модификации), а также порчи или уничтожения.
- Данное понятие также связано с распространением разного рода компьютерных вирусов. В свою очередь **«санкционированный доступ»** – это доступ к объектам, программам и данным пользователей, имеющих право выполнять определённые действия (чтение, копирование и др.), а также полномочия и права пользователей на использование ресурсов и услуг, определённых администратором вычислительной системы.

- Вирусы появились в результате создания самозапускающихся программ.
- **Вирусы** – это класс программ, незаконно проникающих в компьютеры пользователей и наносящих вред их программному обеспечению, информационным файлам и даже техническим устройствам, например, жёсткому магнитному диску. В России вирусы появляются в 1988 году. С развитием сетевых информационных технологий вирусы стали представлять угрозу огромному количеству пользователей сетевых и локальных компьютерных систем.

Современные угрозы информационной безопасности в России

- Согласно Закону о безопасности под угрозой безопасности понимается *совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.*

Современные угрозы информационной безопасности в России

Концепция национальной безопасности РФ не дает определения угрозы, но называет некоторые из них в информационной сфере. Так, опасность представляют:

– 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 несанкционированного доступа к ним.

Современные угрозы информационной безопасности в России

Это так называемые внешние угрозы, которые обусловлены конкурентным характером 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.

Современные угрозы информационной безопасности в России

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.

Современные угрозы информационной безопасности в России

Промышленный шпионаж представляет собой несанкционированную передачу конфиденциальной 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, перехват сообщений, представленных на различных носителях (магнитные носители, письма и др.).

Современные угрозы информационной безопасности в России

Что касается **анализа полученной информации** , то все осталось без изменений. Им занимается человек или группа людей, осуществляющих аналитико-синтетическую переработку информации, в том числе с использованием новых информационных технологий.

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.

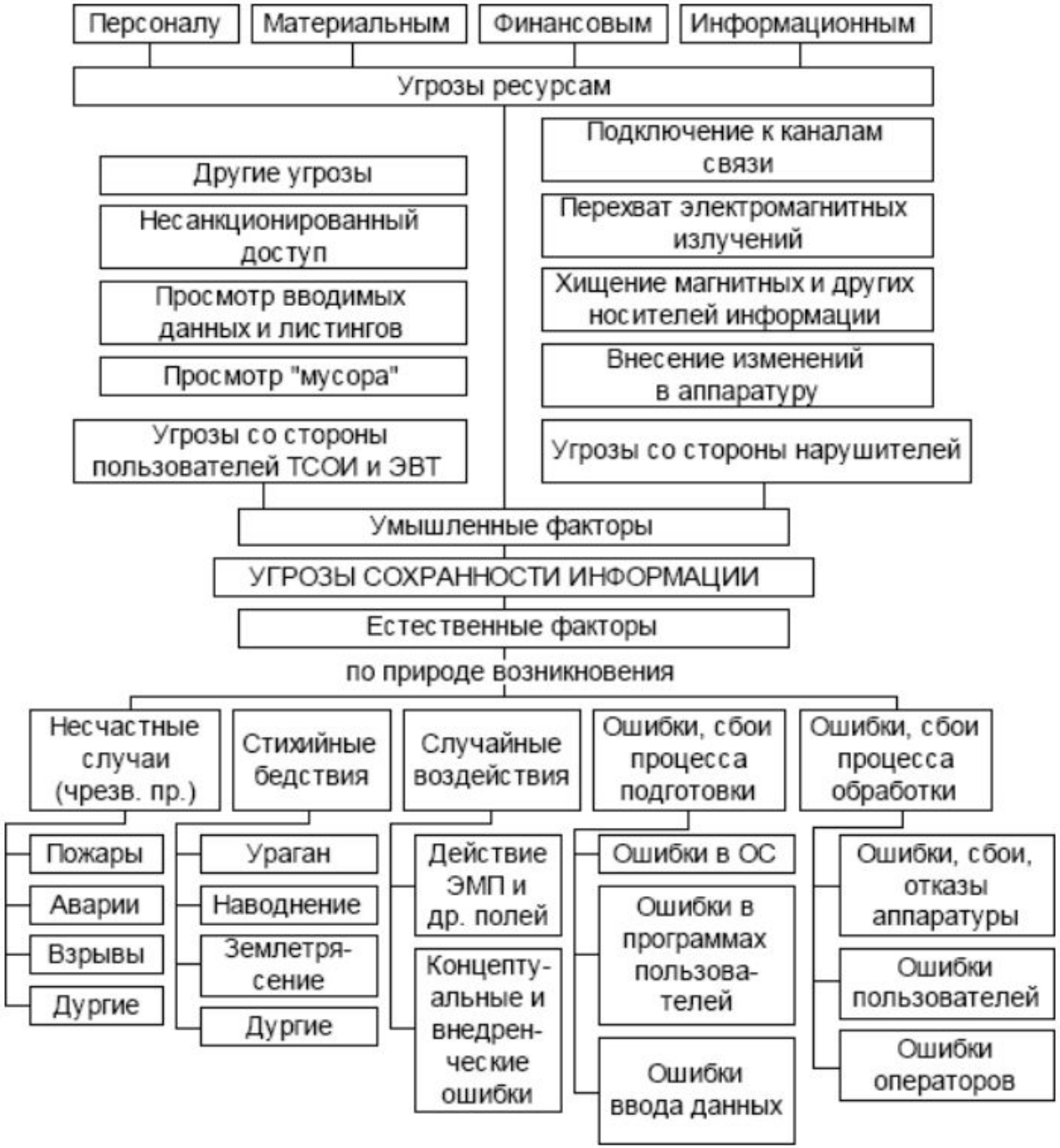

Рис. 1. Классификация угроз безопасности

- В силу изменения концепции развития стратегических вооружений, определяющей, что вооруженное решение мировых проблем становится невозможным, все более прочно входит в обиход понятие **информационной войны.** Сейчас эффективность наступательных средств информационной войны, информационного оружия превосходит эффективность систем защиты информации.

Представляют интерес угрозы утраты охраняемых сведений в ходе информационных процессов, участники которых представляют противоположные интересы. Анализ этих угроз позволил выявить ряд их характерных признаков. В большинстве случаев активные действия сторон вполне осознанны и целенаправленны. К таким действиям относятся:

– разглашение конфиденциальной информации ее обладателем;

– утечка информации по различным, главным образом техническим, каналам;

– несанкционированный доступ к конфиденциальной информации различными способами.

- ***Разглашение информации*** *– это умышленные или неосторожные действия должностных лиц и граждан, которым в установленном порядке были доверены соответствующие сведения по работе, приведшие к оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам*

Как правило, факторами, способствующими разглашению конфиденциальной информации, являются:

– слабое знание (или незнание) требований по защите конфиденциальной информации;

– ошибочность действий персонала из-за низкой производственной квалификации;

– отсутствие системы контроля за оформлением документов, подготовкой выступлений, рекламы и публикаций;

– злостное, преднамеренное невыполнение требований по защите коммерческой тайны.

Разглашение конфиденциальной информации неизбежно приводит к материальному и моральному ущербу.

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 информации характеризуется как обстоятельствами происхождения, так и причинами, условиями возникновения утечки

Кроме того, утечке информации способствуют стихийные бедствия, катастрофы, неисправности, отказы, аварии технических средств и оборудования.

- ***Уничтожение*** *– это противоправное действие, направленное на нанесение материального и информационного ущерба конкуренту со стороны злоумышленника .*
- **вероятные источники утечки информации** следующим образом:

– персонал, имеющий доступ к конфиденциальной информации;

– документы , содержащие эту информацию;

– технические средства и системы обработки информации , в том числе линии связи, по которым она передается.

Основные средства и методы защиты информации

Средства и методы защиты информации обычно делят на две большие группы: организационные и технические.

Под организационными подразумеваются законодательные, административные и физические, а **под техническими** – аппаратные, программные и криптографические мероприятия, направленные на обеспечение защиты объектов, людей и информации.

Программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

С целью организации защиты объектов используют **системы охраны** и **безопасности объектов** – это совокупность взаимодействующих радиоэлектронных приборов, устройств и электрооборудования, средств технической и инженерной защиты, специально подготовленного персонала, а также транспорта, выполняющих названную функцию. При этом используются различные методы, обеспечивающие санкционированным лицам доступ к объектам и ИР. К ним относят аутентификацию и идентификацию пользователей.

Программные и технические средства защиты

Программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

Программные и технические средства защиты

Для **защиты машин от компьютерных вирусов**, профилактики и «лечения» используются программы-антивирусы, а также средства диагностики и профилактики, позволяющие не допустить попадания вируса в компьютерную систему, лечить заражённые файлы и диски, обнаруживать и предотвращать подозрительные действия. Антивирусные программы оцениваются по точности обнаружения и эффективному устранение вирусов, простое использование, стоимость, возможности работать в сети.

Общие выводы

Важно знать, что характерной особенностью электронных данных является возможность легко и незаметно искажать, копировать или уничтожать их. Поэтому необходимо организовать безопасное функционирование данных в любых информационных системах, т.е. защищать информацию.

Защищённой называют информацию, не изменившую в процессе передачи, хранения и сохранения достоверность, полноту и целостность данных.

Несанкционированные воздействия на информацию, здания, помещения и людей могут быть вызваны различными причинами и осуществляться с помощью разных методов воздействия. Подобные действия могут быть обусловлены стихийными бедствиями (ураганы, ливни, наводнения, пожары, взрывы и др.), техногенными катастрофами, террористическими актами и т.п. Борьба с ними обычно весьма затруднена из-за в значительной степени непредсказуемости таких воздействий.

Наибольший ущерб информации и информационным системам наносят неправомерные действия сотрудников и компьютерные вирусы. Для защиты информации в компьютерах и информационных сетях широко используются разнообразные программные и программно-технические средства защиты. Они включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения.

Контрольные вопросы

1. Что такое компьютерный вирус?
2. Назначение компьютерного вируса?
3. Типы вирусов.
4. Программные средства защиты – антивирусные программы (характеристика).
5. Безопасность программно-технических средств и информационных ресурсов (характеристика).
6. Программная защита от несанкционированных воздействий.
7. Криптография, криптографическая защита от несанкционированных воздействий (характеристика).
8. Что такое электронная подпись?
9. Физическая и техническая защита от несанкционированных воздействий (характеристика).
10. Воздействия на здания, помещения, личную безопасность пользователя и обслуживающий персонал.
11. Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации (характеристика).
12. Охрана объектов с целью ограничения свободного доступа, смарткарты и др. (характеристика).