Лекция №1

С.А. Краснов

Основы информационной безопасности

# Основы информационной безопасности

Лекция №1.

Тема №1: Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения.

Тема лекции: Основы информационной безопасности.

**Изучаемые вопросы:**

1. Цели и задачи. Термины и определения.

2. Многообразие понятий «информация» и «информационная безопасность» (ИБ) в контексте современных технических и социотехнических систем, ретроспектива вопроса. Соотношение с англоязычной терминологией.

Целями и задачами освоения темы № 1 «Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения» являются:

• раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности;

• определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации;

• классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

## Термин «информация»

**Информация** [information] — Сведения (сообщения, данные) независимо от формы их представления. Информация в зависимости от категории доступа к ней подразделяется на информацию общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [ N 149-ФЗ ].

1. Форма представления информации может быть классифицирована:

• по степени упорядоченности;

• форме закрепления;

• доступности,

• содержанию,

• затратам интеллектуального труда человека.

**По степени упорядоченности** различают информацию и документированную информацию.

**По форме закрепления** информация подразделяется на представленную в *письменном виде* (рукопись, машинопись, нотная запись и т. д.), в *устной форме* (публичное произнесение, публичное исполнение и т. д.), в *виде звуко- или видеозаписи* (механической, магнитной, цифровой, оптической и т. д.), в *виде изображения* (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео- или фотокадр и т. д.), в *объемно-пространственной форме* (скульптура, модель, макет, сооружение и т. д.).

**По доступности** информация разделяется на *открытую* (общедоступную) и *ограниченного доступа*.

**По содержанию** информация может быть классифицирована по сфере применения; ценности информации от времени; предназначению.

**По сфере применения** информация может быть разделена на экономическую, социально значимую, служебную, частную, развлекательную и тому подобную.

**По ценности информации** от времени информация может быть разделена на *оперативную*, *неоперативную* и *памятники культуры*. Ценность оперативной информации существенно зависит от времени, прошедшего с момента ее возникновения. Ценность неоперативной информации в меньшей степени зависит от времени. Произведения художественной литературы или искусства могут сохранять свою ценность в течение нескольких лет. Если ценность этих произведений не уменьшается в течение десятков лет, они могут быть отнесены к памятникам культуры.

**По предназначению** информация подразделяется на *массовую*, *групповую* и *индивидуальную*. Массовая информация представляет собой сведения, предназначенные для неограниченного круга лиц. Групповая информация ориентирована на использование вполне определенным кругом лиц, имеющих отношение к содержащимся в ней сведениям. Индивидуальная информация ориентирована на конкретного человека.

**По затратам интеллектуального труда человека на создание информации** она условно может быть разделена на высокоинтеллектуальную, распорядительную и бытовую [ Комов-09 ].

## Термин «опасность»

**Опасность** [hazard] — Источник потенциального вреда.

Примечание. Опасность может быть источником риска [ ISO GUIDE 73-2009 ].

**Опасность** — возможность возникновения обстоятельств, при которых материя, поле, энергия, информация или их сочетание могут таким образом повлиять на сложную систему, что приведет к ухудшению или невозможности её функционирования и развития.

**Опасность** — вероятность, возможность того, что может произойти какое-то нежелательное событие.

**Аксиома о потенциальной опасности:** Ни в одном виде деятельности невозможно достичь абсолютной безопасности. Следовательно — любая деятельность потенциально опасна.

**6 этапов в процессе действия опасности:**

1. Источник (субъект) опасности;

• Природные явления (землетрясения, наводнения, засуха и т.д.).

• Элементы техногенной сферы (атомные электростанции, предприятия химической промышленности и др.).

• Человек, группа людей, их сообщество (преступник, преступная организация).

1. Объект, подвергающийся опасности;

• Объектом, подвергающимся опасности, являются люди. Понятие "объект опасности" применительно к чему-либо другому имеет смысл лишь тогда, когда этот объект каким-либо образом включен в жизнь людей и играет в ней важную роль.

1. Средства, которыми источник опасности воздействует на объект опасности;

• В качестве средств воздействия источника опасности выступают те или иные формы насилия, аварии, а также катастрофические природные явления.

1. Цель, которую ставит источник опасности по отношению к объекту;

• Цель, которую преследует источник опасности по отношению к объекту, имеет место только если в качестве источника опасности выступает человек, группа людей или их сообщество.

5. Процесс воздействия источника опасности на объект;

6. Результат воздействия. Результат воздействия источника опасности на объект выражается в следующих формах:

• в утрате объектом тех или иных своих элементов в определенном количестве;

• в нарушении связей между элементами объекта;

• в изменении структуры объекта (изменение формы деятельности);

• в потере способности объекта к развитию;

• в ослаблении функций объекта;

• в полном разрушении объекта.

**Идентификация опасностей:**

Под **идентификацией** (лат. indentifico) понимается процесс обнаружения и установления количественных, временных, пространственных и иных характеристик, необходимых и достаточных для разработки профилактических и оперативных мероприятий, направленных на обеспечение нормального функционирования технических систем и качества жизни. В процессе идентификации выявляются номенклатура опасностей, вероятность их проявления, пространственная локализация (координаты), возможный ущерб и др. параметры, необходимые для решения конкретной задачи.

**Методы обнаружения опасностей** делятся на:

• **инженерный**. Определяют опасности, которые имеют вероятностную природу происхождения.

• **экспертный**. Он направлен на поиск отказов и их причин. При этом создается специальная экспертная группа, в состав которой входят разные специалисты, дающие заключение.

• **социологический** метод. Применяется при определении опасностей путём исследования мнения населения (социальной группы). Формируется путём опросов.

• **регистрационный**. Заключается в использовании информации о подсчете конкретных событий, затрат каких-либо ресурсов, количестве жертв.

• **органолептический**. При органолептическом методе используют информацию, получаемую органами чувств человека (зрением, осязанием, обонянием, вкусом и др.). Примеры применения — внешний визуальный контроль техники, изделия, определение на слух (по монотонности звука) четкости работы двигателя и пр.

**Квантификация опасностей:**

**Квантификация** (лат. quatum — сколько) — количественное выражение, измерение, вводимое для оценки сложных, качественно определяемых понятий.

**Опасности характеризуются** потенциалом, качеством, временем существования или воздействия на человека, вероятностью появления, размерами зоны действия.

Потенциал проявляется с количественной стороны, например уровень шума, запыленность воздуха, напряжение электрического тока.

Качество отражает его специфические особенности, влияющие на организм человека, например частотный состав шума, дисперсность пыли, род электрического тока.

Применяются численные, балльные и другие приемы квантификации.

Мерой опасности может выступать и число пострадавших.

Другой мерой опасности может быть и приносимый её реализацией ущерб для окружающей среды, который только частично может быть измерен экономически (в основном через затраты на ликвидацию последствий).

Наиболее распространенной оценкой является **риск** — вероятность потерь при действиях, сопряженных с опасностями.

## Термин «угроза»

**Угроза** [threat] —

1. Потенциальная возможность нарушения защиты [ ГОСТ Р ИСО 7498-2-99 ].

2. Потенциальная причина инцидента, который может нанести ущерб системе или организации [ ГОСТ Р ИСО/МЭК 13335-1-2006 ].

3. Опасность, предполагающая возможность потерь (ущерба) [ СТО БР ИББС-1.0-2010 ].

4. Потенциальная опасность нарушения одного или нескольких свойств системы криптографической (протокола криптографического), например, конфиденциальности, целостности, аутентификации, невозможности отказа, неотслеживаемости [ Словарь крипт. терминов ].

**Угроза (безопасности информации):**

**Угроза**  [threat] —

1. Совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации и/или воздействиями несанкционированными и/или непреднамеренными на нее [ГОСТ Р 51624-2000], [ ГОСТ Р 53113 ].

2. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или)целостности информации [ Р 50.1.053-2005 ].

3. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [Р 50.1.056-2005], [ ГОСТ Р 50922-2006 ].

**Угроза активная** [active threat] —

1. Угроза преднамеренного несанкционированного изменения состояния системы.

**Примечания:**

1) Примерами активных угроз, относящихся к защите информации, могут служить модификация сообщений, дублирование сообщений, вставка ложных сообщений, маскирование какого-либо логического объекта под санкционированный логический объект и отклонение услуги.

2) Активные угрозы системе означают изменение информации, содержащейся в системе, либо изменения состояния или работы системы. Примером активной угрозы служит умышленное изменение таблиц маршрутизации системы неполномочным пользователем [ ГОСТ Р ИСО 7498-2-99 ].

2. Угроза, которая может быть реализована путем намеренного несанкционированного вмешательства в работу криптосистемы (протокола криптографического) [ Словарь крипт. терминов ].

**Угроза пассивная** [passive threat] —

Угроза несанкционированного раскрытия информации без изменения состояния системы.

Примечание. К пассивным угрозам относятся те, которые при их реализации не приводят к какой-либо модификации любой информации, содержащейся в системе (системах), и где работа и состояние системы не изменяются. Одной из реализаций пассивной угрозы является использование перехвата для анализа информации, передаваемой по каналам связи [ ГОСТ Р ИСО 7498-2-99 ].

**Угроза безопасности информационной** [information security threat] —

1. Фактор или совокупность факторов, создающих опасность функционированию и развитию информационной сферы [ Концепция ИБ ВС ].

2. Угроза нарушения свойств безопасности информационной — доступности, целостности или конфиденциальности активов информационных организации банковской системы Российской Федерации [ СТО БР ИББС-1.0-2010 ].

**Угроза безопасности информационной организации**  —

Совокупность факторов и условий, создающих опасность нарушения безопасности информационной организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Примечание 1. Формой реализации (проявления) угрозы безопасности информационной является наступление одного или нескольких взаимосвязанных событий безопасности информационной и инцидентов безопасности информационной, приводящего(их) к нарушению свойств безопасности информационной объекта(ов) защиты организации.

Примечание 2. Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы [ГОСТ Р 53114-2008].

**Источники и последствия угрозы:**

1. **Источник угрозы** - событие, явление или процесс, который (отдельно или в совокупности с другими источниками) порождает угрозу безопасности.

2. **Последствие угрозы безопасности** - событие, явление или процесс, характеризующий в совокупности с другими событиями, явлениями или процессами состояние и тенденции развития ситуации, возникающий после возможной реализации угрозы.

**Виды взаимосвязей между угрозами, их источниками и последствиями:**

1. Некоторое событие, явление или процесс является источником не одной, а совокупности угроз безопасности.

2. Некоторое событие, явление или процесс может быть последствием реализации не одной, а совокупности угроз безопасности.

3. Источниками угроз безопасности могут быть другие угрозы безопасности или последствия других угроз безопасности.

4. **Последствия угроз** безопасности сами могут представлять собой угрозы безопасности.

**Угроза безопасности информационной взаимоувязанной сети связи Российской Федерации**  —

Последствия воздействия нарушителя безопасности информационной Взаимоувязанной сети связи Российской Федерации, не предотвращение, либо не обнаружение и не ликвидация которого средствами Взаимоувязанной сети связи Российской Федерации может привести к ухудшению заданного Руководящими и нормативными документами уровня качества службы или к ухудшению заданных качественных характеристик функционирования Взаимоувязанной сети связи Российской Федерации и, как следствие, нанесению ущерба пользователю или оператору связи Взаимоувязанной сети связи Российской Федерации [ ОСТ 45.127-99 ].

## Термин «риск»

**Риск** [risk] — **Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы** [ СТО БР ИББС-1.0-2010 ].

1. **Влияние неопределенности на цели**.

Примечание 1. Влияние — это отклонение от того, что ожидается (положительное и/или отрицательное).

Примечание 2. Цели могут иметь различные аспекты (например, финансовые и экологические цели и цели в отношении здоровья и безопасности) и могут применяться на различных уровнях (стратегических, в масштабах организации, проекта, продукта или процесса).

Примечание 3. Риск часто характеризуется ссылкой на потенциально возможные события и последствия или их комбинации.

Примечание 4. Риск часто выражают в виде комбинации последствий событий (включая изменения в обстоятельствах) и их возможности.

Примечание 5. Неопределенность — это состояние, заключающееся в недостаточности, даже частичной, информации, понимания или знания относительно события, его последствий или его возможности [ ISO GUIDE 73-2009 ].

2. **Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов**.

Примечание. Определяется как сочетание вероятности события и его последствий [ ГОСТ Р ИСО/МЭК 13335-1-2006 ].

3. **Влияние неопределенностей на процесс достижения поставленных целей**.

Примечание 1. Цели могут иметь различные аспекты: финансовые, аспекты, связанные со здоровьем, безопасностью и внешней средой, и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса.

Примечание 2. Риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а также на то, как они могут влиять на достижение целей.

Примечание 3. Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности [ГОСТ Р 53114-2008].

4. **Влияние неопределенности на цели организации**.

Примечание 1. Влияние неопределенности подразумевает отклонение от ожидаемого результата.

Примечание 2. Цели организации могут иметь различные аспекты (финансовые аспекты,аспекты, связанные с охраной здоровья, безопасностью и внешней средой) и могут применяться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта или процесса.

Примечание 3. Риск часто характеризуют ссылкой на потенциальные события, их последствия или их комбинацию, а также на то, как они могут влиять на достижение целей организации.

Примечание 4. Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и связанной с ними вероятностью их возникновения [ГОСТ Р 53131-2008].

**Риск нарушения безопасности информационной** — риск, связанный с угрозой безопасности информационной [ СТО БР ИББС-1.0-2010 ].

**Риск остаточный** [residual risk] —

1. Риск, остающийся после обработки риска [ГОСТ Р ИСО/МЭК 27001-2006].

2. Риск, сохраняющийся после воздействия на риск.

Примечание 1. Риск остаточный может содержать в себе неидентифицированный риск.

Примечание 2. Риск остаточный может быть также известен как «удержанный риск» [ ISO GUIDE 73-2009 ].

3. Риск, остающийся после его обработки [ ГОСТ Р ИСО/МЭК 13335-1-2006 ].

**Менеджмент риска** [risk management] —

Полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий [ ГОСТ Р ИСО/МЭК 13335-1-2006 ].

**Менеджмент безопасности информационной организации** [management] —

Скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации [ГОСТ Р 53114-2008].

## Термин «безопасность»

**Безопасность** [security] —

1. Свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение [ Комов-09 ].

2. Состояние защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз [ СТО БР ИББС-1.0-2010 ].

**Безопасность информации (данных)** [data security] —

1. Состояние защищенности информации (данных), обрабатываемой средствами вычислительной техники или системы автоматизированной, от угроз внутренних или внешних [ РД Защита от НСД ].

2. Состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность [ ГОСТ Р 50922-2006 ].

3. Состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

Примечание. Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии [ Р 50.1.053-2005 ].

**Безопасность информационная международная** —

Состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве [ Доклад Ген. секретаря ООН от 10 июня 2000 г. ].

**Безопасность информации (при применении информационных технологий)** — Состояние защищенности технологии информационной, обеспечивающее безопасность информации, для обработки которой она применяется, и безопасность информационной системы автоматизированной информационной, в которой она реализована [ Р 50.1.053-2005 ].

**Безопасность информационная** [information security] —

1. Обобщенный термин для обозначения состояния защищенности и области деятельности по обеспечению безопасности ресурсов информационных. В общем случае информация может быть представлена в любой форме: печатной, электронной и т. д. В широком смысле включает самые разнообразные аспекты б. и.: защита информации, безопасность компьютерная и сетевая, безопасность систем информационно-телекоммуникационных, безопасность систем информационных, безопасность технологий информационных, безопасность информационно-психологическая и др.

2. Состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность.

3. Обеспечение конфиденциальности, доступности и целостности информации; дополнительно могут подразумеваться другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность [ISO/IEC 17999: 2005].

4. Защита конфиденциальности, целостности и доступности информации [ГОСТ Р ИСО/МЭК 17799-2005].

5. Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки [ ГОСТ Р ИСО/МЭК 13335-1-2006 ].

6. Безопасность, связанная с угрозами в сфере информационной.

Примечание. Защищенность достигается обеспечением совокупности свойств безопасности информационной — доступности, целостности, конфиденциальности активов информационных. Приоритетность свойств безопасности информационной определяется ценностью указанных активов для интересов (целей) организации банковской системы Российской Федерации [ СТО БР ИББС-1.0-2010 ].

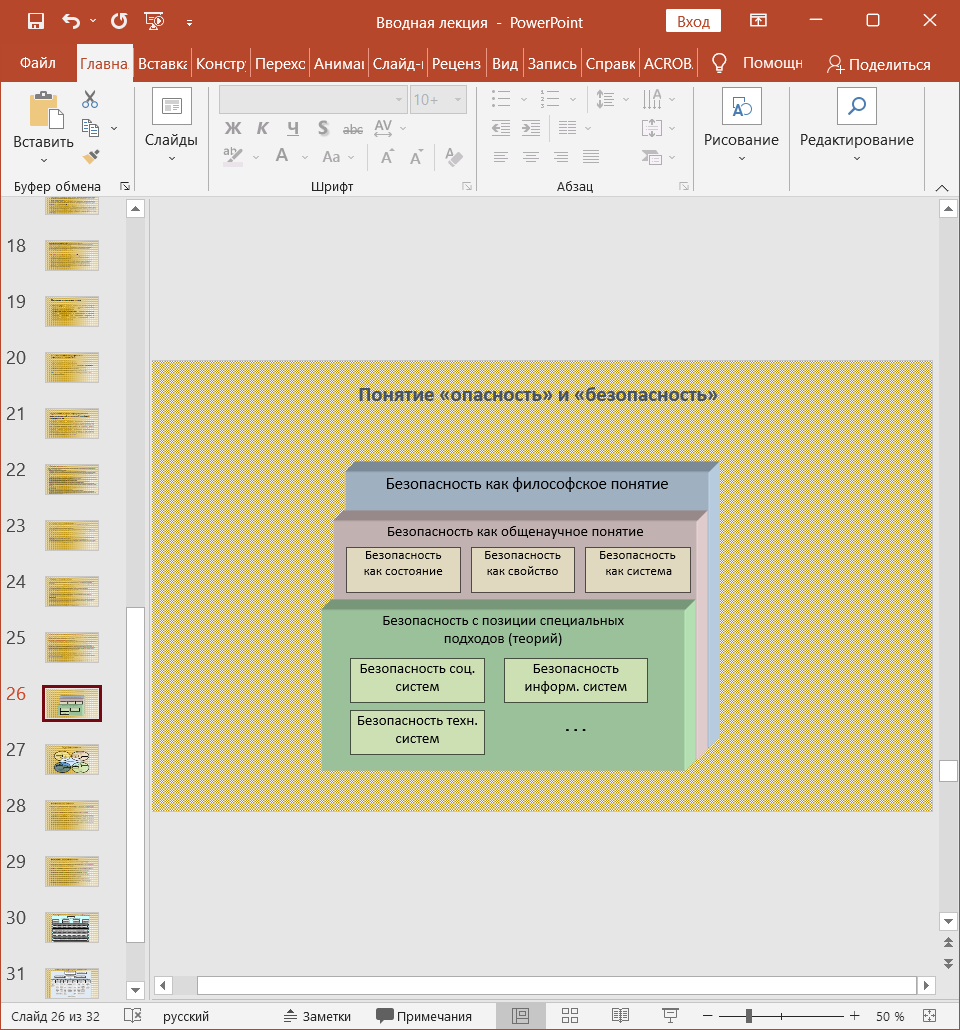


Рисунок – Понятие «опасность» и «безопасность»

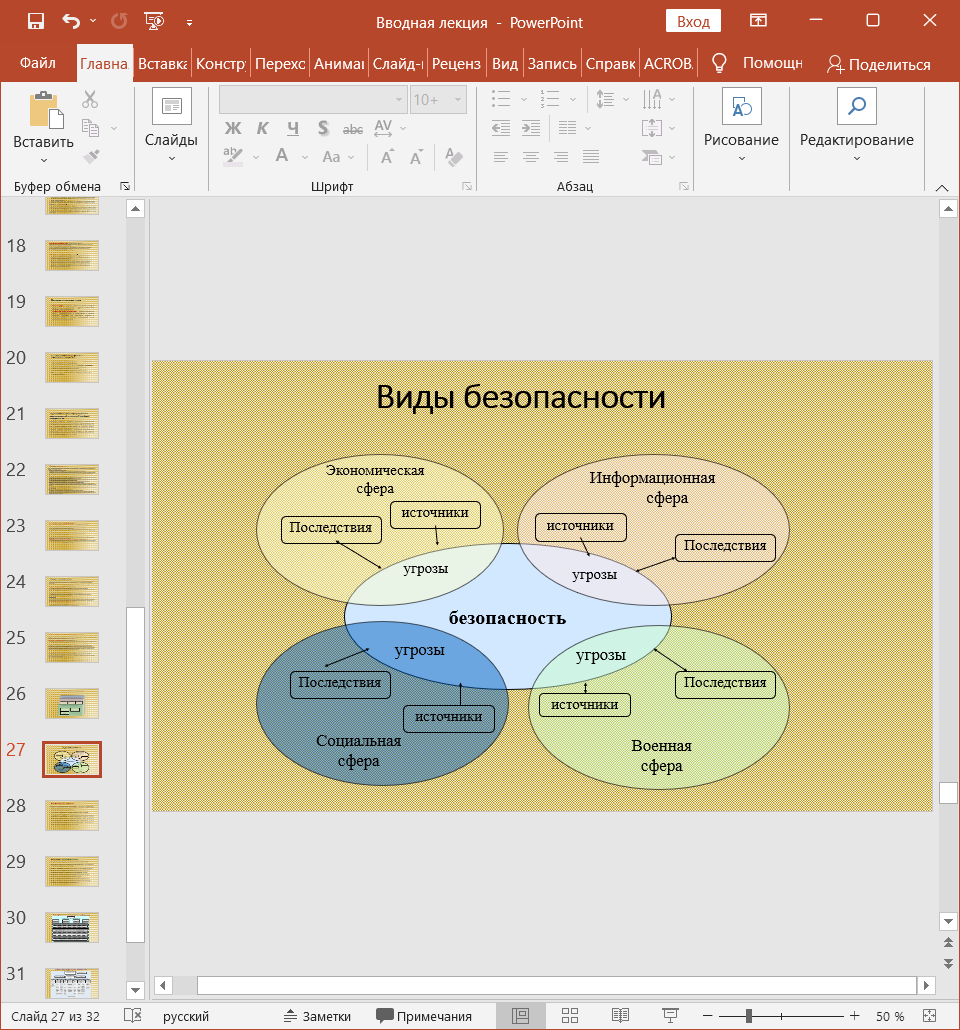


Рисунок – Виды безопасности

**Система комплексной безопасности:**

Совокупность организационных мероприятий и действий подразделений охраны и служб безопасности организаций и автоматизированных систем по защите информации, направленных на:

• обеспечение установленного режима, порядка и правил поведения;

• предотвращение, обнаружение и ликвидацию угроз жизни, среде обитания, имуществу и информации, а также поддержание работоспособности технических средств и систем, на охраняемом объекте с целью ограничения или предотвращения действий нарушителя для осуществления опасных несанкционированных операций на объекте, приводящих к частичному или полному нарушению функционирования объекта.

**Задачи системы обеспечения безопасности:**

• Своевременное прогнозирование и выявление внешних и внутренних угроз.

• Осуществление комплекса оперативных и долговременных мер по предупреждению и нейтрализации внутренних и внешних угроз.

• Создание и поддержание в готовности сил и средств для обеспечения безопасности.

• Управление силами и средствами обеспечения безопасности в нормальных (повседневных) условиях и при возникновении чрезвычайных ситуаций.

• Осуществление системы мер по нормальному функционированию объектов безопасности после возникновения чрезвычайных ситуаций.

• Участие в мероприятиях по обеспечению безопасности за пределами своего объекта в соответствии с договоренностями (соглашениями), например внутри корпорации или объединения фирм (предприятий) и т.д.



Рисунок – Государственная система защиты информации



Рисунок – Типовая структура службы безопасности