Лекция №2

С.А. Краснов

Нормативно-правое регулирование в области информационной безопасности

# Нормативно-правое регулирование в области информационной безопасности

Лекция №2.

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

Тема лекции: Нормативно-правое регулирование в области информационной безопасности.

**Изучаемые вопросы:**

1. Правовое регулирование в области ИБ.

2. Модель эшелонированной обороны. Важность и сложность проблемы информационной безопасности.

## Понятие информационной безопасности (ИБ)

Один из основных документов, регламентирующих понятие безопасности – Указ Президента Российской Федерации от 31 декабря 2015 года N 683. "**О Стратегии национальной безопасности Российской Федерации**".

I. Общие положения

II. Россия в современном мире

III. Национальные интересы и стратегические национальные приоритеты

IV. Обеспечение национальной безопасности

Оборона страны

Государственная и общественная безопасность

Повышение качества жизни российских граждан

Экономический рост

Наука, технологии и образование

Здравоохранение

Культура

Экология живых систем и рациональное природопользование

Стратегическая Стабильность и равноправное стратегическое партнерство

V. Организационные, нормативно-правовые и информационные основы реализации настоящей Стратегии

VI. Основные показатели состояния национальной безопасности

Суть стратегии национальной безопасности РФ, а также ряд определений:

Настоящая Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

**Национальная безопасность Российской Федерации** (далее - национальная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации.

Национальная безопасность **включает** в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, ***информационную***, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

**Национальные интересы Российской Федерации** (далее - национальные интересы) объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития;

**Угроза национальной безопасности** - совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам;

**Обеспечение национальной безопасности** - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

**Стратегические национальные приоритеты Российской Федерации** (далее - стратегические национальные приоритеты) - важнейшие направления обеспечения национальной безопасности;

**Система обеспечения национальной безопасности** совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов.

В Доктрине информационной безопасности Российской Федерации термин "*информационная безопасность*" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере.

I. **Общие положения**

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В настоящей Доктрине под ***информационной сферой*** понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением ***информационной безопасности***, а также совокупность механизмов регулирования соответствующих общественных отношений.

II. **Национальные интересы в информационной сфере**

III. **Основные информационные угрозы и состояние информационной безопасности**

IV. **Стратегические цели и основные направления обеспечения информационной безопасности**

V. **Организационные основы обеспечения информационной безопасности**

**В Доктрине используются следующие основные понятия:**

а) **угроза информационной безопасности РФ** (далее - информационная угроза) - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

б) **информационная безопасность РФ** (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства;

в) **обеспечение информационной безопасности** - осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно- технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) **силы обеспечения информационной безопасности** - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством РФ задач по обеспечению ИБ;

е) **средства обеспечения информационной безопасности** - правовые, организационные, технические и другие средства, используемые силами обеспечения ИБ;

ж) **система обеспечения информационной безопасности** - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения ИБ;

В Законе РФ "Об участии в международном информационном обмене" *информационная безопасность* определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В рамках данного курса под **информационной безопасностью** будем понимать защищенность 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, рисунок 1.

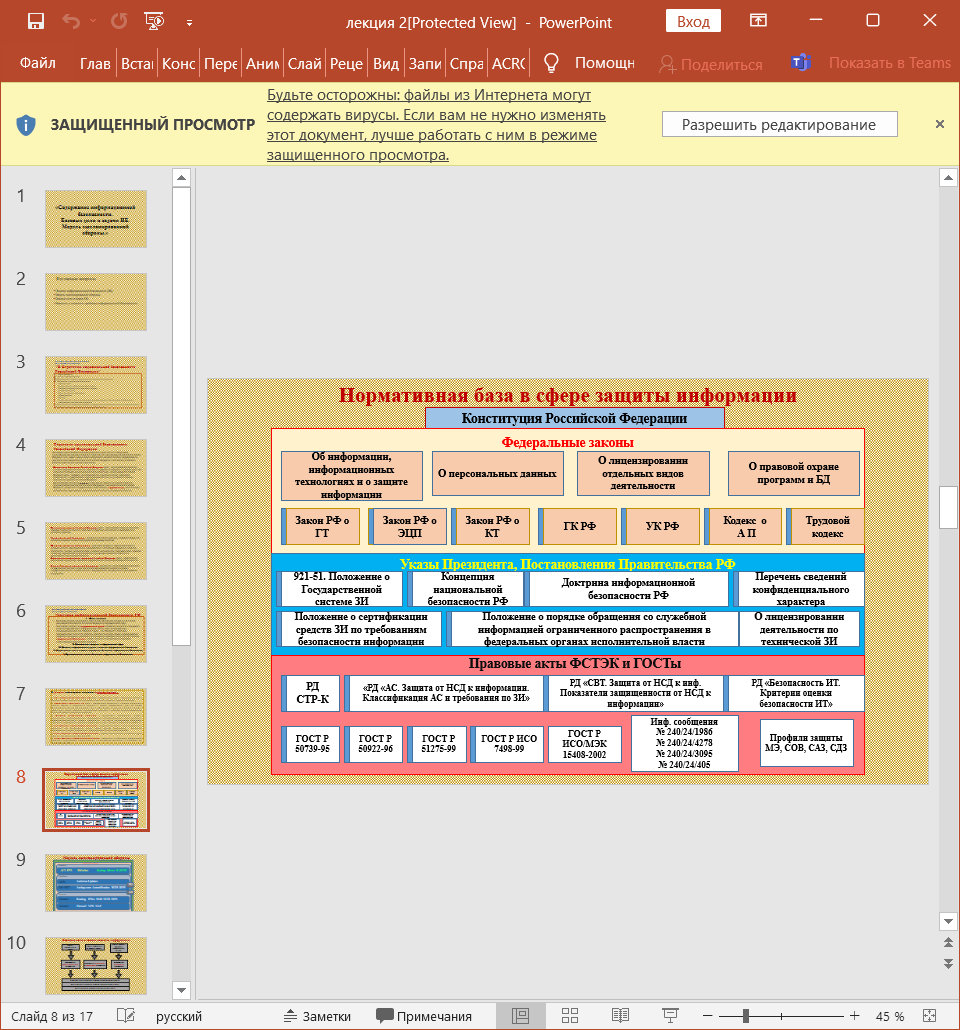


Рисунок 1

**Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

**Защита информации** (*ГОСТ Р 50922-2006г.*) – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности **нарушитель** необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т. д.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться.

*Например*, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Исходя из этого, отметим следующее:

— задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

— информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

В ряде случаев понятие "*информационная безопасность*" подменяется термином "*компьютерная безопасность*". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.

В рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

## Модель эшелонированной обороны

С развитием информационных технологий, всё больше возникало проблем с информационной безопасностью, а, следовательно, всё больше появлялось решений, которые с этим связаны. Сегодня существует множество моделей, позволяющие упорядочить ситуацию в этой области (рисунок 2).

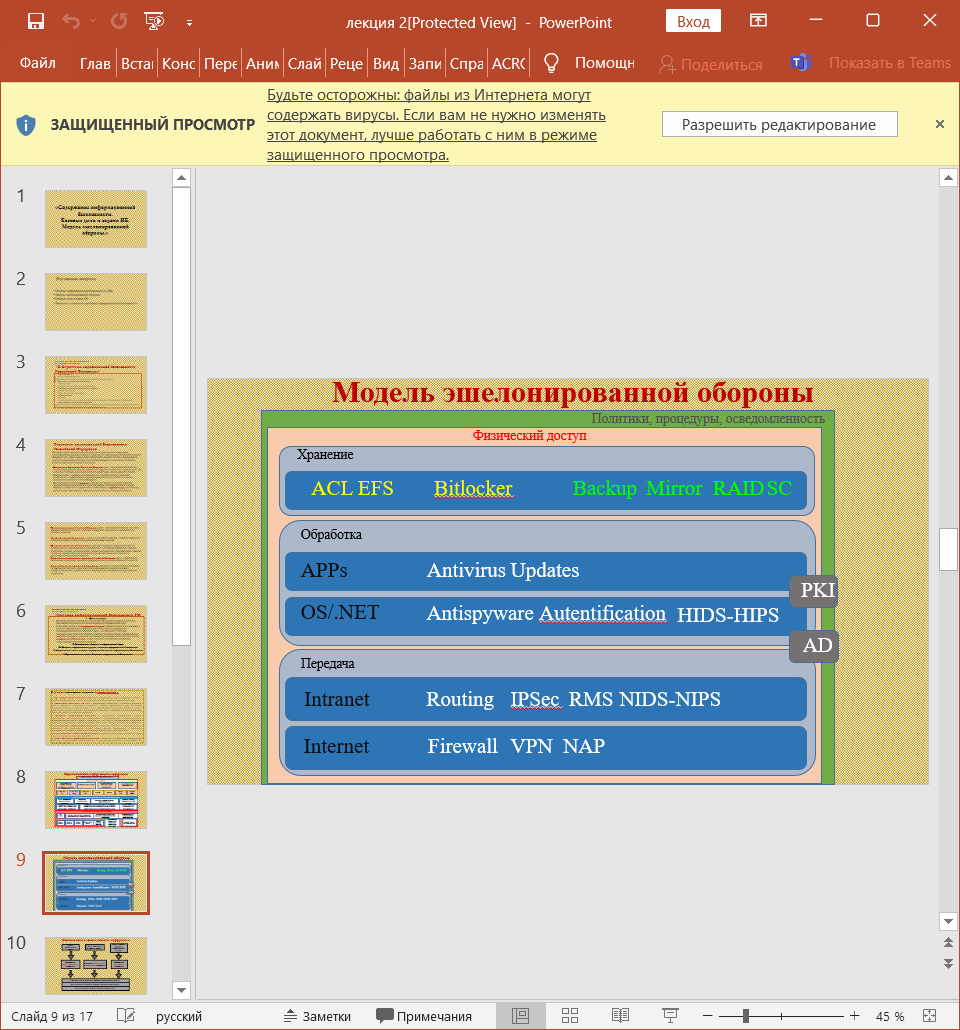


Рисунок 2

Одна из них, под названием «*Модель эшелонированной обороны*» («Defense in Depth»), предложена Агентством национальной безопасности США, а компания Microsoft её применила к компьютерной среде. Схема модели эшелонированной обороны представлена на слайде.

В основе модели лежит пришедший из военной науки тезис о том, что в обороне никогда нельзя ограничиваться только одним эшелоном, причём эшелоны должны быть разные. Достаточно вспомнить фортификационные сооружения средних веков – расчищенное от леса пространство, ров, крепостная стена, внутренняя стена, башня-донжон. И на каждом уровне – разное оружие.

В информационной системе то же самое. В **качестве уровней** – **состояния информации**, в которых она существует в информационных системах: хранение, обработка, передача.

В качестве видов оружия – различные технологии, каждая из которых использует свои, характерные только для неё, способы обеспечения безопасности.

Плюс технологии, которые лежат в основе целого ряда инструментов, непосредственно работающих с информацией. Конечно, без качественной технологии обработки металла не удастся создать ни нормального ружья, ни танка.

Так и здесь – *службы каталогов сетевых ресурсов* (в инфраструктуре Microsoft эту роль исполняет Active Directory) и *инфраструктура работы с открытыми ключами* (PKI) лежат в основе целого ряда технологий разных уровней.

Тем не менее, технологии используют **люди**. Существует оценка, по которой до 80 % угроз информационной безопасности предприятию исходят от персонала этого предприятия. Есть целая наука – *социальная инженерия* (Social Engineering), которая изучает методы того, как заставить человека выполнить то, что нужно. И здесь не брезгают ничем, начиная с горячего утюга и прямого подкупа, однако наибольшее внимание сосредоточивается на способах, с помощью которых можно так заставить человека выполнить действия, наносящие непоправимый ущерб родному предприятию, что он об этом даже не догадается.

*BitLocker* (для Windows) позволяет защищать данные путём полного шифрования диска(ов).

*ACL* (Access Control List) — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают.

*EFS* (Encrypting file system) - Шифрующая файловая система это тесно интегрированная с NTFS служба, располагающаяся в ядре Windows.

*Apps* - *applications*, дословно, приложения.

*RMS* (Rights Management Services) - технология защиты документов Microsoft Active Directory путем шифрования.

*NIDS-NIPS* - два типа систем предотвращения вторжений. Решения NIPS анализируют трафик, прежде чем пропустить его в сеть или подсеть. Решения HIPS анализируют пакеты перед тем, как они поступают в компьютер.

*NAP* - технология компании Microsoft, предназначенная для контроля доступа к сети предприятия.

## Базовые цели и задачи ИБ.

Для эффективного использования модели прежде всего нужно определить проблемы, связанные с её использованием. Точнее – *свойства информации*, соблюдение адекватного состояния которых и определяет её безопасность.

Приведем базовые цели и задачи защиты информации (рисунок 3).

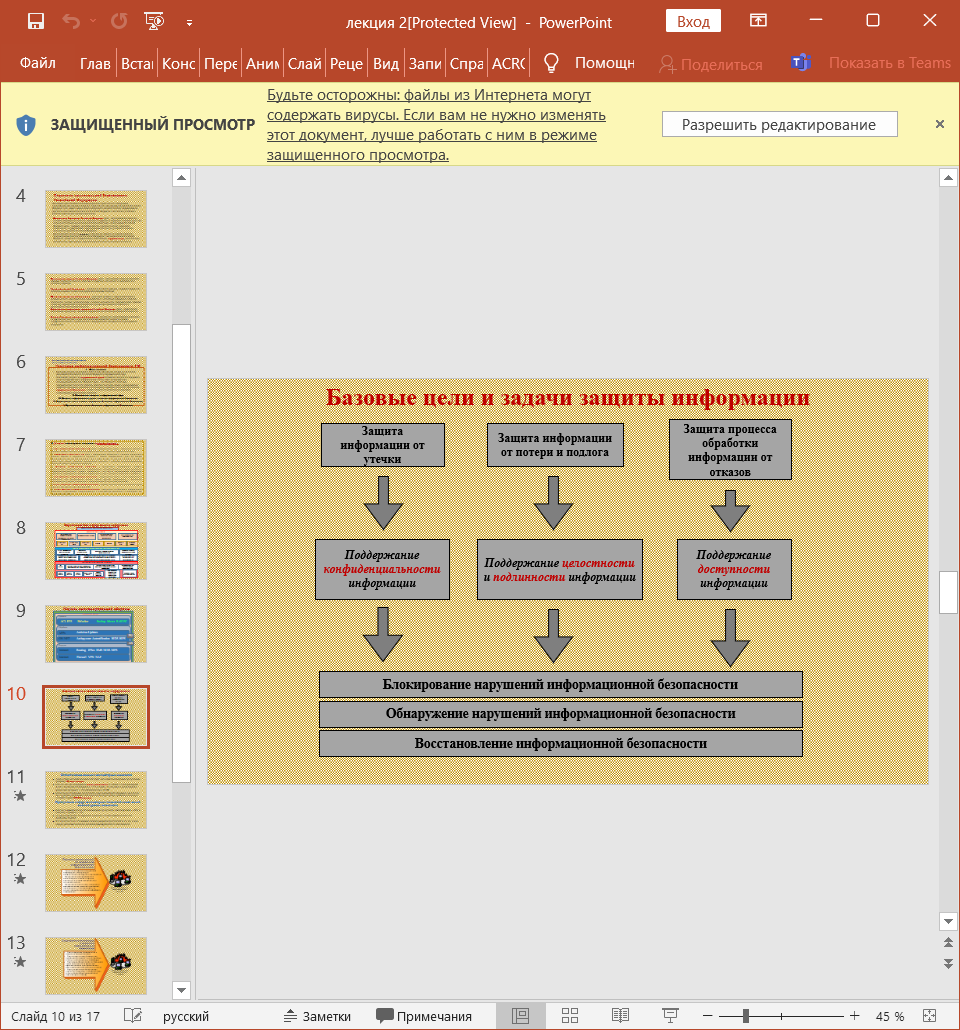


Рисунок 3

Именно **доступность, целостность и конфиденциальность** являются равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

**Конфиденциальность** – это защита от несанкционированного доступа к информации.

В соответствии с руководящими документами ФСТЭК под поддержанием конфиденциальности информации понимается ее доступность только для тех лиц, которые имеют на это соответствующие полномочия.

Под **целостностью** – понимается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Целостность информации условно подразделяется на *статическую* и *динамическую*. *Статическая целостность* информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. *Динамическая целостность* информации включает вопросы корректного выполнения сложных действий с информационными потоками (транзакций).

В соответствии с руководящими документами ФСТЭК под поддержанием целостности информации понимается ее *неизменность* (физическая целостность) и *непротиворечивость* (логическая целостностью) в процессе хранения и передачи.

**Доступность** – это возможность за приемлемое время получить требуемую информационную услугу. Существует классификация уровней доступности: немедленная доступность, доступность в ограниченное время, доступность в разумное время.

Так же в рамках доступности не лишним будет вспомнить о ***надежности*** технического устройства (аппаратного или программного) - его способность точно, своевременно и корректно выполнять все свои функции при нормальных условиях функционирования.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом (рисунок 4). Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

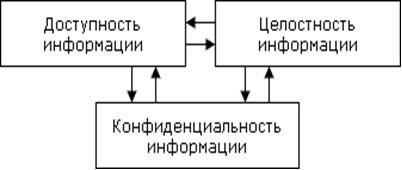


Рисунок 4

Таким образом, обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

— обеспечением доступности информации;

— обеспечением целостности информации;

— обеспечением конфиденциальности информации.

## Важность и сложность проблемы информационной безопасности.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасности есть составная часть информационных технологий - области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса. Статистические данные о компьютерных инцидентах:

— Только в США ежегодный экономический ущерб, наносимый компьютерными преступниками, превышает **150 млрд. долларов**.

— В России ежегодно возбуждаются **тысячи уголовных дел** по статьям 272 («Неправомерный доступ к компьютерной информации»), 273 («Создание, использование и распространение вредоносных программ") и 159 («Мошенничество») УК РФ.

— Количество регистрируемых преступлений в сфере компьютерной информации, как в России, так и за рубежом представляет собой неуклонно растущую кривую, динамика роста которой составляет порядка **300-400% ежегодно**.

**Преступления в сфере компьютерных технологий имеют самый высокий уровень латентности:**

— В России не выявляется более 90% компьютерных преступлений, в Великобритании — 85%, в США 80%, в Германии — 75%.

— До суда доходят меньше 3% нарушений, а ревизия в состоянии выявить не более 10% электронных хищений.

— Рост преступности на 2-3% вызывает снижение раскрытия преступлений на 1%, что, в свою очередь, увеличивает количество уклонения правонарушителей от ответственности.

Несмотря на совершенствование технологий в области информационно-компьютерной безопасности уязвимость компьютерных систем продолжает возрастать.

Причины:

1. Общие предпосылки, связанные с ростом усилий по нарушению информационной безопасности:



Рисунок 5 – Общие предпосылки, связанные с ростом усилий по нарушению информационной безопасности

2. Современные тенденции в развитии компьютерных технологий:



Рисунок 6 – Современные тенденции в развитии компьютерных технологий

3. Недостатки компьютерных систем:



Рисунок 7 – Недостатки компьютерных систем

4. Отсутствие системного подхода к решению проблемы информационно-компьютерной безопасности:



Рисунок 8 – Отсутствие системного подхода к решению проблемы информационно-компьютерной безопасности

Таким образом мы подходим к необходимости защиты информации, методы ее защиты представлены на рисунке 9.



Рисунок 9

## Вопросы

1. В чем заключается проблема информационной безопасности?

2. Дайте определение понятию "информационная безопасность".

3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?

4. Что понимается под "компьютерной безопасностью"?

5. Приведите определение доступности информации.

6. Приведите определение целостности информации.

7. Приведите определение конфиденциальности информации.

8. Предпосылки, связанные с ростом усилий по нарушению информационной безопасности.

9. Недостатки компьютерных систем.