Лекция 2. Угрозы. Модель угроз.

Болатбек М.А.

С конца 80-ых, начале 90-х годов проблемы, связанные с защитой информации беспокоят как специалистов в области компьютерной безопасности, так и многочисленных рядовых пользователей персональных компьютеров. Это связано с глубокими изменениями, вносимыми компьютерной технологией в нашу жизнь. Современные автоматизированные информационные системы (АИС) в экономике – сложные механизмы, состоящие из большого количества компонентов различной степени автономности, связанных между собой и обменивающихся данными. Практически каждый из них может выйти из строя или подвергнуться внешнему воздействию.

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа защищаемым данным.

Под угрозой безопасности информации (информационной угрозой) понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства. Если ценность информации теряется при ее хранении и/или распространении, то реализуется угроза нарушения конфиденциальности информации.

Если информация изменяется или уничтожается с потерей ее ценности, то реализуется угроза целостности информации. Если информация вовремя не поступает легальному пользователю, то ценность ее уменьшается и со временем полностью обесценивается, тем самым угроза оперативности использования или доступности информации

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов иногда преподносимых самой природой.

ИЗ-ЗА ЧЕГО ВОЗНИКАЮТ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

Невнимательность сотрудников

Использование пиратского ПО

Distributed-Denial-of-Service-атака (хакерская атака)

Вирусы

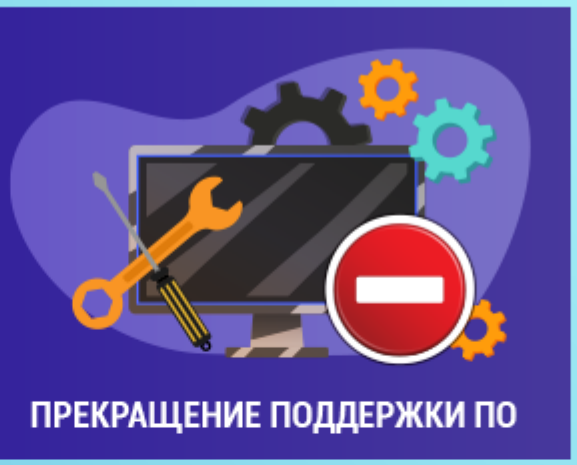
Утечка информации со стороны работников и совладельцев бизнеса

Вмешательство госорганов

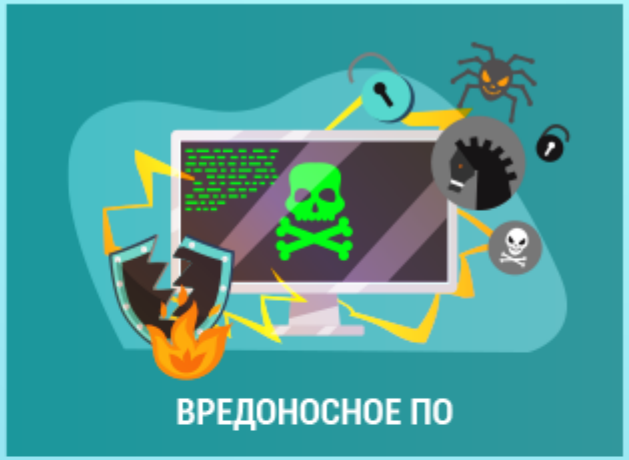
НАИБОЛЕЕ ОПАСНЫЕ УГРОЗЫ ИБ


Угрозы информационной безопасности
Для государства
Для компаний (юридических лиц)
Для физических лиц
Информационные войны
Разглашение
Киберслежка
Кибератаки
Утечка
Мошенничество
Кибершпионаж
Несанкционированный доступ
Фишинг, вишинг, фарминг
Киберпреступность, кибертерроризм
Распространение секретной информации

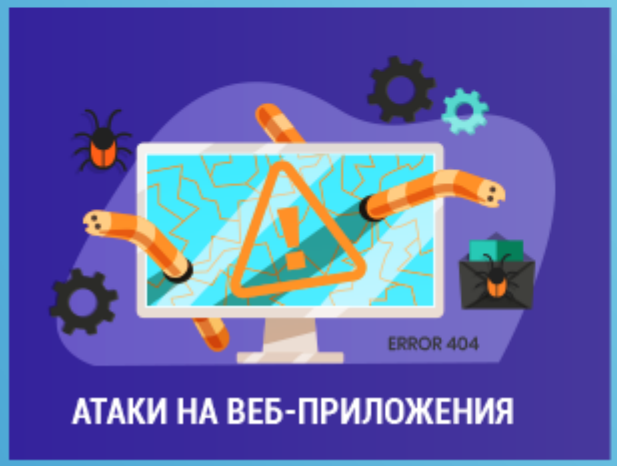
DDOS-АТАКИ



ПРЕКРАЩЕНИЕ ПОДДЕРЖКИ ПО



ВРЕДОНОСНОЕ ПО



АТАКИ НА ВЕБ-ПРИЛОЖЕНИЯ

УТЕЧКИ ДАННЫХ

БЛОКИРОВКА SSL-СЕРТИФИКАТОВ

Информационные угрозы могут быть обусловлены: естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины); человеческими факторами. Последние, в свою очередь, подразделяются на:

– угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

– угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной "утечкой умов", знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на внутренние, возникающие внутри управляемой организации, и внешние. Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем. основным угрозам безопасности относят:

раскрытие конфиденциальной информации;

компрометация информации;

несанкционированное использование информационных ресурсов; ошибочное использование ресурсов;

несанкционированный обмен информацией;

отказ от информации;

отказ от обслуживания

Средствами реализации угрозы раскрытия конфиденциальной информации могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации. Реализация угроз является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации (106). При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом.

Умышленные или неосторожные действия сотрудников, приведшие к ознакомлению с КИ недопущенных лиц

Выражается в:
– сообщении;
– передаче;
– предоставлении;
– пересылке;
– опубликовании;
– утере
И иных способах
Реализуется по каналам распространения и СМИ

Бесконтрольный выход КИ за пределы организации или круга лиц, которым она была доверена

Возможна по каналам:
– визуально-оптическим;
– акустическим;
– электромагнитным;
– материально-вещественным

Противоправное преднамеренное ознакомление с КИ недопущенных лиц. Нарушение целостности и доступа к защищаемой информации

Реализуется способами:
– сотрудничество;
– склонение к сотрудничеству;
– выведывание;
– подслушивание;
– наблюдение;
– хищение;
– копирование;
– подделка;
– уничтожение;
– подключение;
– перехват;
– негласное ознакомление;
– фотографирование;
– сбор и аналитическая обработка

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием: разглашения конфиденциальной информации; ухода информации по различным, главным образом техническим, каналам; несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям. Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам. По физической природе возможны следующие средства переноса информации:

Световые лучи.

Звуковые волны.

Электромагнитные волны.

Материалы и вещества

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника. Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

визуально-оптические;

акустические (включая и акустико-преобразовательные);

электромагнитные (включая магнитные и электрические);

материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида – твердые, жидкие, газообразные).

Несанкционированный доступ (НСД) Это наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный». По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам. Есть и достаточно примитивные пути несанкционированного доступа:

хищение носителей информации и документальных отходов;

инициативное сотрудничество;

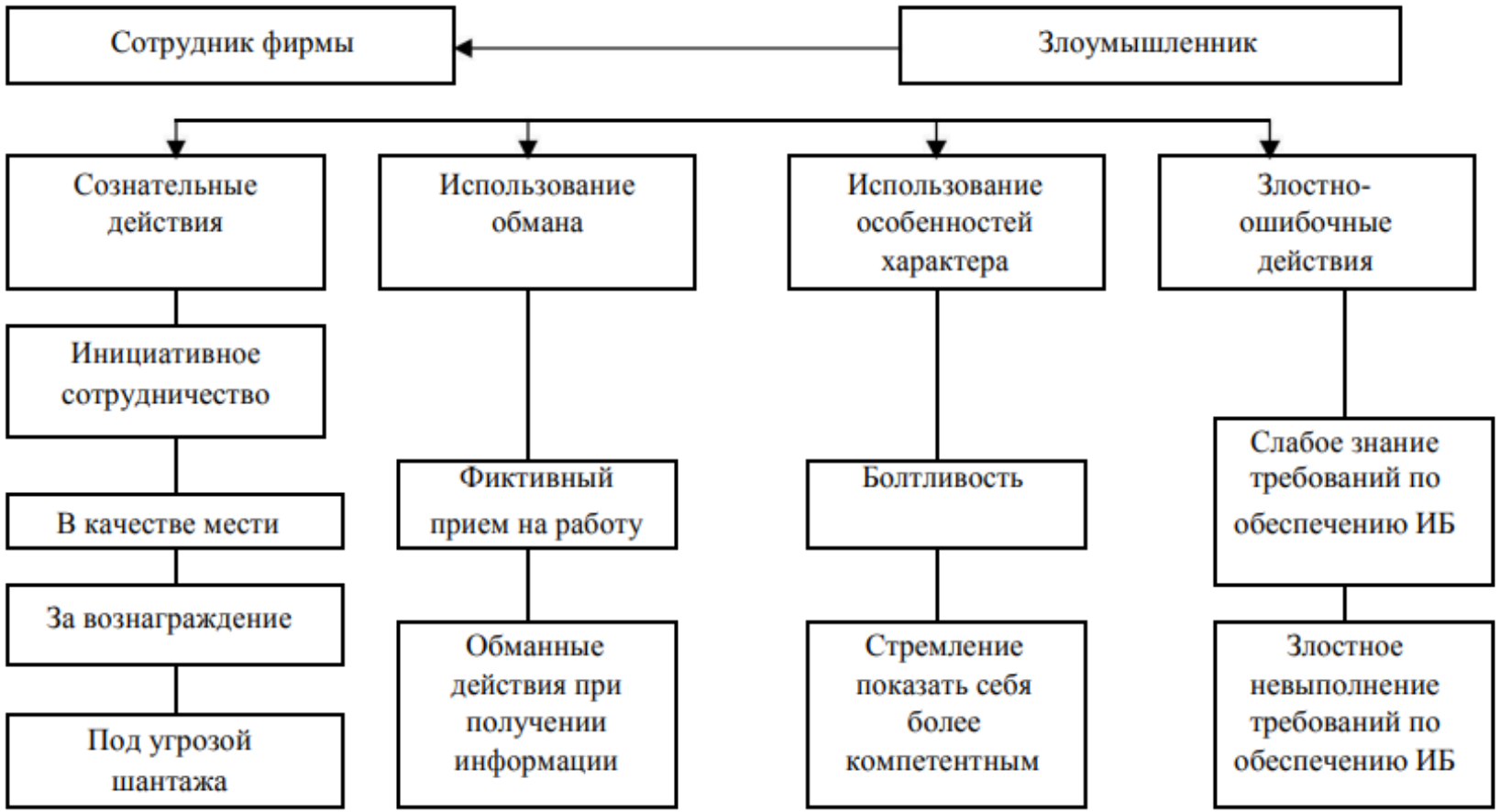
склонение к сотрудничеству со стороны взломщика;

выпытывание;

подслушивание;

наблюдение и другие пути.

Разглашение и утечка приводит к неправомерному ознакомлению с конфиденциальной информацией при минимальных затратах усилий со стороны злоумышленника. Этому способствуют некоторые не лучшие личностно-профессиональные характеристики и действия сотрудников фирмы



Уничтожение компьютерной информации – это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание (например, введение ложной информации, добавление, изменение, удаление записей). Одновременный перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен. Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени.

Блокирование компьютерной информации – это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями. Отказ от информации, в частности, непризнание транзакции (операции в банке) состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения "техническим" путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Модификация компьютерной информации – это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных. Адаптация программы для ЭВМ или базы данных – «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя. Другими словами это означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя

Копирование компьютерной информации – изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИС. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных действий

Способы воздействия угроз на информационные объекты подразделяются на:

– информационные;

– программно-математические;

– физические;

– радиоэлектронные;

– организационно-правовые.

К информационным способам относятся:

– нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

– несанкционированный доступ к информационным ресурсам;

– манипулирование информацией (дезинформация, сокрытие или сжатие информации);

– нарушение технологии обработки информации.

Программно-математические способы включают:

– внедрение компьютерных вирусов;

– установка программных и аппаратных закладных устройств;

– уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

– уничтожение или разрушение средств обработки информации и связи;

– уничтожение, разрушение или хищение машинных или других носителей информации;

– хищение программных или аппаратных ключей и средств криптографической защиты информации;

– воздействие на персонал;

– перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;

– воздействие на парольно-ключевые системы;

– радиоэлектронное подавление линий связи и систем управления.

Радиоэлектронными способами являются:

– перехват информации в технических каналах ее возможной утечки;

– внедрение электронных устройств перехвата информации в технические средства и помещения;

– перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;

– воздействие на парольно-ключевые системы;

– радиоэлектронное подавление линий связи и систем управления

Организационно-правовые способы включают:

– невыполнение требований законодательства о задержке в принятии необходимых нормативно-правовых положений в информационной сфере;

– неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Суть подобных угроз сводится, как правило, к нанесению того или иного ущерба предприятию. Проявления возможного ущерба могут быть самыми различными:

моральный и материальный ущерб деловой репутации организации; моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

моральный и материальный ущерб от дезорганизации в работе всего предприятия.

Непосредственный вред от реализованной угрозы, называется воздействием угрозы.

Идентификация угроз предполагает рассмотрение воздействий и последствий от реализации угроз. Обычно воздействие угроз приводит к раскрытию, модификации, разрушению информации или отказу в информационном обслуживании. Более значительные долговременные последствия реализации угрозы приводят к потере бизнеса, нарушению тайны, гражданских прав, потере адекватности данных, потере человеческой жизни и иным долговременным эффектам.

Знание возможных угроз, а также уязвимых мест защиты, необходимо, чтобы выбрать наиболее экономичные средства обеспечения безопасности. Самыми частыми и опасными, с точки зрения размеров ущерба, являются не угрозы даже, а непреднамеренные ошибки пользователей, операторов, системных администраторов и других, обслуживающих информационные системы лиц. Иногда такие ошибки являются угрозами (неправильно преднамеренно введенные данные, ошибки в программе), а иногда это просто следствие человеческих слабостей, которыми, однако, могут воспользоваться злоумышленники – таковы обычно ошибки администрирования, 65% потерь –следствие непреднамеренных ошибок

Угрозы, исходящие от окружающей среды, весьма разнообразны. В первую очередь следует выделить нарушение инфраструктуры - аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки и т. п. На долю огня, воды и аналогичных "врагов", среди которых самый опасный - низкое качество электропитания, приходится 13% потерь, которые обычно несут информационные системы.

Внешние субъекты могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

криминальные структуры;

потенциальные преступники и хакеры;

недобросовестные партнеры;

технический персонал поставщиков услуг;

представители надзорных организаций и аварийных служб;

представители силовых структур.

Внутренние субъекты, как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

основной персонал (пользователи, программисты, разработчики);

представители службы защиты информации;

вспомогательный персонал (уборщики, охрана);

технический персонал (жизнеобеспечение, эксплуатация).

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

средства связи;

сети инженерных коммуникаций (водоснабжения, канализации);

транспорт.

Внутренними источниками потенциальных угроз безопасности информации могут быть:

аппаратно- программные средства;

некачественные технические средства обработки информации;

некачественные программные средства обработки информации;

вспомогательные технические средства (охраны, сигнализации, телефонии);

другие технические средства, применяемые в учреждении.

Активное воздействие всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. На основе такого рода анализа можно иногда получить довольно интересную информацию. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка. Такая ошибка может быть обусловлена одной из следующих причин:

– неадекватностью политики безопасности реальной системе. Это означает, что разработанная политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий;

– ошибками административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной организации. Например, согласно политике безопасности должен быть запрещен доступ пользователей к определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям.

– ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программы или комплекса программ и благодаря которым их можно использовать совсем не так, как описано в документации. Примером такой ошибки может служить ошибка в программе аутентификации пользователя, когда при помощи определенных действий пользователь имеет возможность войти в систему без пароля.

– ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или о

Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ системы хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавление программ в АИСЭО без разрешения администратора безопасности системы.

В последнее время участились случаи воздействия на вычислительную систему при помощи специально созданных программ. Под вредоносными программами в дальнейшем будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

«Троянский конь» – программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Аналогия древнегреческим «троянским конем» таким образом вполне оправдана – в не вызывающей подозрений оболочке таится угроза. Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователем. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне).

Наиболее опасные действия «троянский конь» может выполнять, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнить несанкционированные привилегированные функции чужими руками. Или, например, злоумышленника очень интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий – это не помешает выполнению несанкционированных действий

Вирус – это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению.

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия. Процесс заражения вирусом программных файлов можно представить следующим образом. В зараженной программе код последней изменяется таким образом, чтобы вирус получил управление первым, до начала работы программы вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы. Если вирус записывается в конец программы, то он корректирует код программы с тем, чтобы получить управление первым. После этого управление передается программе-вирусоносителю, и та нормально выполняет свои функции. Более изощренные вирусы могут для получения управления изменять системные области накопителя (например, сектор каталога), оставляя длину и содержимое заражаемого файла без изменений.

Загрузочные вирусы. От файловых вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей (гибких и жестких дисков). На включенном компьютере они могут временно располагаться в оперативной памяти.

Обычно поражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус. Так, например, при попытке загрузить компьютер с гибкого диска происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд. В частности, к таким документам относятся документы текстового процессора Microsoft Word. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

«Червь» – программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

«Жадные» программы – это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Естественно, такая атака будет активным вмешательством в работу системы. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода.

Захватчики паролей. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом - с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Незаконное использование привилегий

Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение (системное или прикладное), функционирующее в нештатном режиме. Практически любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, при сбоях оборудования или средства, которые способны функционировать с нарушением существующей политики безопасности. В некоторых случаях пользователь должен иметь возможность доступа ко всем наборам системы (например, при внезапной проверке). Такие средства необходимы, но они могут быть чрезвычайно опасными. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции

Для того чтобы уменьшить риск от применения таких средств большинство систем защиты реализует такие функции с помощью набора привилегий – для выполнения определенной функции требуется определенная привилегия. В этом случае каждый пользователь получает свой набор привилегий, обычные пользователи – минимальный, администраторы – максимальный (в соответствии с принципом минимума привилегий).

Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты (что, например, оказалось возможным в одной из версий операционной системы UNIX), либо в случае халатности при управлении системой и привилегиями в частности (например, при назначении расширенного набора привилегий всем подряд).

Атаки «салями» более всего характерны для систем, обрабатывающих денежные счета и, следовательно, для банков особенно актуальны. Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы. Например, 6,5% годовых от $102,87 за 31 день составит $0,5495726. Банковская система может округлить эту сумму до $0.55. Однако если пользователь имеет доступ к банковским счетам или программам их обработки, он может округлить ее в другую сторону – до $0.54, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент, при обработке 10.000 счетов в день. Его прибыль таким образом составит $1000, т.е. около $300 000 в год

«Скрытые каналы» – пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. Практически любое действие в системе каким-то образом затрагивает другие ее элементы, которые при этом могут изменять свое состояние. При достаточной наблюдательности и знании этих связей можно получить прямой или опосредованный доступ к данным. «Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»).

Например, программист банка не всегда имеет доступ к именам и балансам депозитных счетов. Программист системы, предназначенной для обработки ценных бумаг, может не иметь доступ к предложениям о покупке или продаже. Однако при создании таких систем он может предусмотреть способ получения интересующих его сведений. В этом случае программа скрытым способом устанавливает канал связи с этим программистом и сообщает ему требуемые сведения.

Под «маскарадом» понимается выполнение каких-либо действий одним пользователем от имени другого пользователя. При этом такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Цель «маскарада» – сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий. «Маскарад» – это способ активного нарушения защиты системы, он является опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей.

Примером «маскарада» может служить вход в систему под именем и паролем другого пользователя, при этом система защиты не сможет распознать нарушение. В этом случае «маскараду» обычно предшествует взлом системы или перехват пароля.

Другой пример «маскарада» – присвоение имени другого пользователя в процессе работы. Это может быть сделано с помощью средств операционной системы (некоторые операционные системы позволяют изменять идентификатор пользователя в процессе работы) или с помощью программы, которая в определенном месте может изменить определенные данные, в результате чего пользователь получит другое имя. В этом случае «маскараду» может предшествовать захват привилегий, или он может быть осуществлен с использованием какой-либо ошибки в системе.

«Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы сети. Особенно это касается управляющих сообщений, изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций.

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к огромным убыткам.

Особенно это касается платежей с помощью электронных банковских карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери кредитной карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т.д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей.

«Сборка мусора»

После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя прочитать такие данные трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации

«Взлом системы»

Под «взломом системы» понимают умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем (паролями). «Взлом системы» – умышленное, активное воздействие на систему в целом. «Взлом системы» обычно происходит в интерактивном режиме. Поскольку имя пользователя не является секретом, объектом «охоты» обычно становится пароль. Способы вскрытия пароля могут быть различны: перебор возможных паролей, «маскарад» с использованием пароля другого пользователя, захват привилегий. Кроме того, «взлом системы» можно осуществить, используя ошибки программы входа

«Люки»

Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом. Сущность использования люков состоит в том, что при выполнении пользователем некоторых не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности - выход в привилегированный режим).

«Люки» чаще всего являются результатом забывчивости разработчиков. В частности, отладка программы ведется за счет прямого доступа к отдельным частям продукта или наборе определенного сочетания клавиш.

Одним из наиболее показательных примеров использования «забытых» люков является, пожалуй, широко известный в компьютерном мире вирус Морриса. Одной из причин, обусловивших возможность распространения этого вируса, была ошибка разработчика программы электронной почты. По оценкам американских специалистов, ущерб нанесенный в результате этого инцидента, составил более чем 100 миллионов долларов.

Основные классы вирусов

Среда обитания:	Сетевые	Распространяются по компьютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Способы заражения

Резидентные	Находятся в памяти, активны до выключения компьютера
Нерезидентные	Не заражают память, являются активными ограниченное время
Безвредные	Практически не влияют на работу; уменьшают свободную память на диске в результате своего размножения
Неопасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты
Опасные	Могут привести к потере программ или системных данных
Очень опасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты

Особенности алгоритма вируса

Вирусы-«спутники»	Вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением .com
Вирусы-«черви»	Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса
«паразитические»	Изменяют содержимое дисковых секторов или файлов
«стелс»-вирусы («невидимки»)	Перехватывают обращения операционной системы к пораженным файлам или секторам и подставляют вместо себя незараженные участки
Вирусы-призраки	Не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано
Макровирусы	Пишутся не в машинных кодах, а на WordBasik, живут в документах Word, переписывают себя в Normal.dot

Безопасность

Разрабатывая своё приложение, стоит задумываться о его безопасности. Веб-безопасности. Не хотелось бы, чтобы в одно прекрасное утро на сайте появилась надпись «Hacked by %hackername%» на белом фоне или же чтобы все содержимое сайта, включая персональные данные пользователей ушли в чужие руки.

Общесетевые атаки (legacy)

- **Фишинг (phishing)** - вид атаки, который начинается с рассылки почтовых сообщений, содержащих ссылку на известный ресурс (или имитирующий такую ссылку). Дизайн веб-страницы обычно копируется с воспроизводимого ресурса.
- **Спуфинг (spoofing)** - одна из разновидностей фишинга. Ее суть заключается в атаке через DNS (или каким-то иным способом), когда страница с известным URL подменяется страницей злоумышленника.
- **Социальная инженерия** - это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.
- **Троянский конь (Spyware)** - программа, записывающая все нажатия клавиш на терминале или мышке, способна записывать screenshot'ы и передавать эти данные удаленному хозяину.

Аутентификация (Authentication)

- Подбор (Brute Force)

автоматизированный процесс проб и ошибок, использующийся для того, чтобы угадать имя пользователя, пароль, номер кредитной карточки, ключ шифрования и т.д.

- Недостаточная аутентификация (Insufficient Authentication)

эта уязвимость возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации

- Небезопасное восстановление паролей (Weak Password Recovery Validation)

эта уязвимость возникает, когда Web-сервер позволяет атакующему несанкционированно получать, модифицировать или восстанавливать пароли других пользователей

Авторизация (Authorization)

- Предсказуемое значение идентификатора сессии (Credential/Session Prediction)

предсказуемое значение идентификатора сессии позволяет перехватывать сессии других пользователей

- Недостаточная авторизация (Insufficient Authorization)

недостаточная авторизация возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям, доступ к которым должен быть ограничен

- Отсутствие таймаута сессии (Insufficient Session Expiration)

в случае если для идентификатора сессии или учетных данных не предусмотрен таймаут или его значение слишком велико, злоумышленник может воспользоваться старыми данными для авторизации

- Фиксация сессии (Session Fixation)

используя данный класс атак, злоумышленник присваивает идентификатору сессии пользователя заданное значение

Атаки на клиентов (Client-side Attacks)

- Подмена содержимого (Content Spoofing)

используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированны Web-сервером, а не переданы из внешнего источника

- Межсайтовое выполнение сценариев (Cross-site Scripting, XSS)

наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя

- Расщепление HTTP-запроса (HTTP Response Splitting)

при использовании данной уязвимости злоумышленник посылает серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа

Выполнение кода (Command Execution)

- Переполнение буфера (Buffer Overflow)

эксплуатация переполнения буфера позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы

- Атака на функции форматирования строк (Format String Attack)

при использовании этих атак путь исполнения программы модифицируется методои перезаписи областей памяти с помощью функций форматирования символьных переменных

- Выполнение команд ОС (OS Commanding)

атаки этого класса направлены на выполнение команд операционной системы на Web-сервере путем манипуляции входными данными

- Внедрение операторов SQL (SQL Injection)

эти атаки направлены на Web-серверы, создающие SQL запросы к серверам СУБД на основе данных, вводимых пользователем

- Внедрение серверных сценариев (SSI Injection)

атаки данного класса позволяют злоумышленнику передать исполняемый код, который в дальнейшем будет выполнен на Web-сервере

Разглашение информации (Information Disclosure)

- Индексирование директорий (Directory Indexing)

атаки данного класса позволяют атакующему получить информацию о наличии файлов в Web каталоге, которые недоступны при обычной навигации по Web сайту

- Идентификация приложений (Web Server/Application Fingerprinting)

определение версий приложений используется злоумышленником для получения информации об используемых сервером и клиентом операционных системах, Web-севераx и браузерах

- Утечка информации (Information Leakage)

эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы

- Обратный путь в директориях (Path Traversal)

данная техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера.

- Предсказуемое расположение ресурсов (Predictable Resource Location)

позволяет злоумышленнику получить доступ к скрытым данным или функциональным возможностям

Логические атаки (Logical Attacks)

- Злоупотребление функциональными возможностями (Abuse of Functionality)

данные атаки направлены на использование функций Web-приложения с целью обхода механизмов разграничение доступа

- Отказ в обслуживании (Denial of Service)

данный класс атак направлен на нарушение доступности Web-сервера

- Недостаточное противодействие автоматизации (Insufficient Anti-automation)

эти уязвимости возникаеют, в случае, если сервер позволяет автоматически выполнять операции, которые должны проводиться вручную

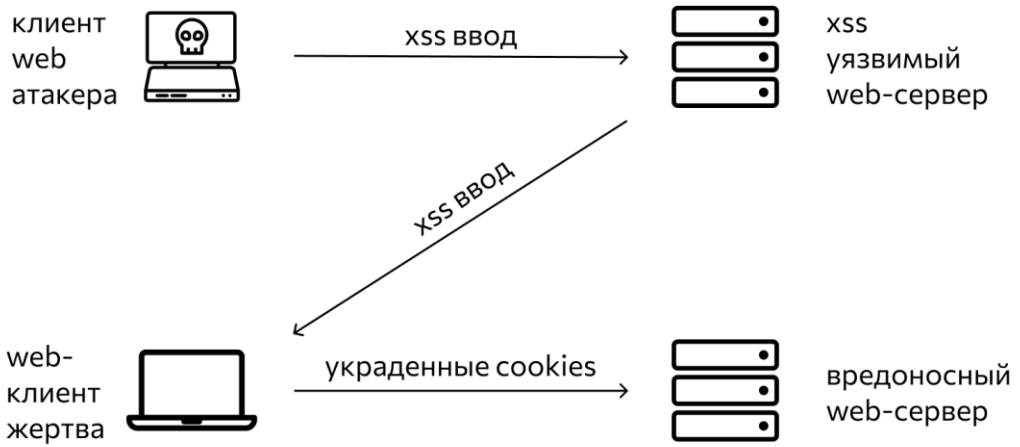
- Недостаточная проверка процесса (Insufficient Process Validation)

уязвимости этого класса возникают, когда сервер недостаточно проверяет последовательность выполнения операций приложения

Угрозы безопасности сайта

Межсайтовый скриптинг (XSS)

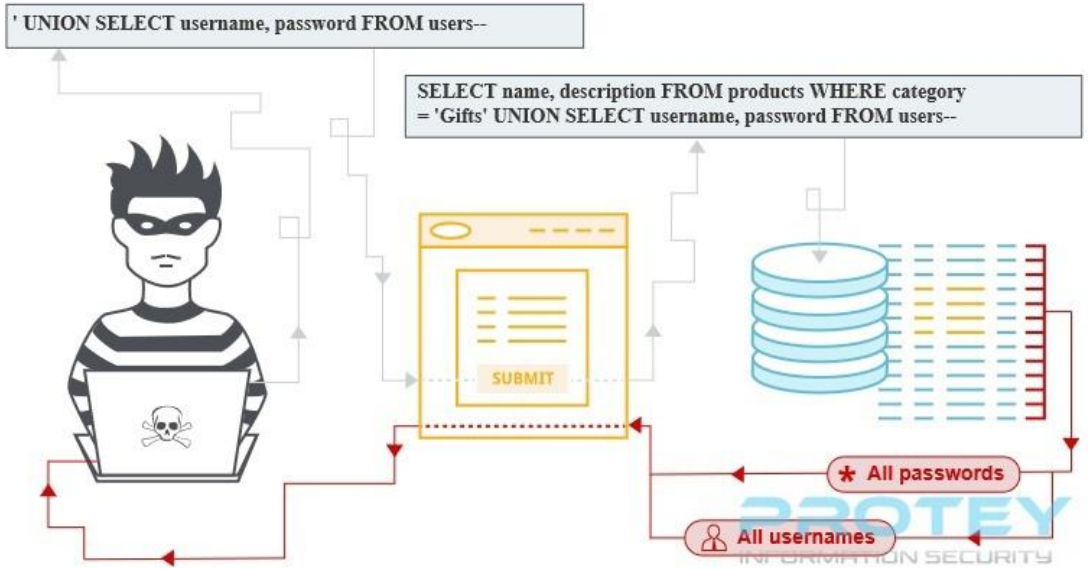
XSS (*Cross-Site Scripting* - Межсайтовый скриптинг) это термин, используемый для описания типа атак, которые позволяют злоумышленнику внедрять вредоносный код *через* веб-сайт в браузеры других пользователей. Поскольку внедрённый код поступает в браузер с сайта, он является *доверенным* и может выполнять такие действия, как отправка авторизационного файла *cookie* пользователя злоумышленнику. Когда у злоумышленника есть файл *cookie*, он может войти на сайт, как если бы он был пользователем, и сделать все, что может пользователь, например, получить доступ к данным кредитной карты, просмотреть контактные данные или изменить пароли.



SQL injection

Уязвимости SQL-инъекций позволяют злоумышленникам выполнять произвольный код SQL в базе данных, позволяя получать, изменять или удалять данные независимо от разрешений пользователя. Успешная инъекционная атака может подделать удостоверения, создать новые удостоверения с правами администратора, получить доступ ко всем данным на сервере или уничтожить / изменить данные, чтобы сделать их непригодными для использования.

Типы внедрения SQL включают внедрение SQL на основе ошибок, внедрение SQL на основе логических ошибок и внедрение SQL на основе времени.



Эта уязвимость присутствует, если пользовательский ввод, который передаётся в базовый оператор SQL, может изменить смысл оператора. Например, следующий код предназначен для перечисления всех пользователей с определённым именем (userName), которое было предоставлено из формы HTML:

```
statement = "SELECT * FROM users WHERE name = '" + userName + "';"
```

Если пользователь указывает реальное имя, оператор будет работать так, как задумано. Однако злонамеренный пользователь может полностью изменить поведение этого оператора SQL на новый оператор в следующем примере, просто указав текст полужирным шрифтом для userName.

```
SELECT * FROM users WHERE name = 'a';DROP TABLE users; SELECT * FROM userinfo WHERE 't' = 't';
```

Модифицированный оператор создаёт действительный оператор SQL, который удаляет таблицу пользователей и выбирает все данные из таблицы userinfo (которая раскрывает информацию о каждом пользователе). Это работает, потому что первая часть введённого текста (a ';) завершает исходное утверждение.
Чтобы избежать такого рода атак, вы должны убедиться, что любые пользовательские данные, которые передаются в запрос SQL, не могут изменить природу запроса. Один из способов сделать это - экранировать все символы пользовательского ввода, которые имеют особое значение в SQL.

Угрозы кибербезопасности АС

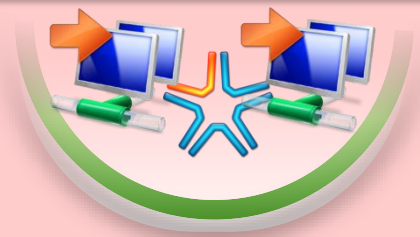
Средства

- Вирусы, черви, троянские программы и другие программные средства;
- Суперкомпьютеры;
- Средства сбора, обработки и передачи информации;
- Компьютерные сети, бот-сети, средства телекоммуникаций, электронные СМИ.

Уязвимости

- систем энергоснабжения;
- каналов связи, полей радиообмена, РЭС;
- аппаратных средств;
- общесистемного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- прикладного программного обеспечения (в том числе средств защиты информации);
- носителей информации;
- персонала.

Угрозы



- безопасности информации, обрабатываемой и передаваемой
- функционированию средств и систем передачи и обработки данных;
- функционированию систем защиты информации и вычислительной техники;
- связанные с ошибками и недостатками проектирования и эксплуатации элементов АС;
- персоналу и пользователям АС;
- правильности принятия решений;
- нарушения порядка управления;
- информационному и программному взаимодействию внутри АС.

Критически важные информационные системы

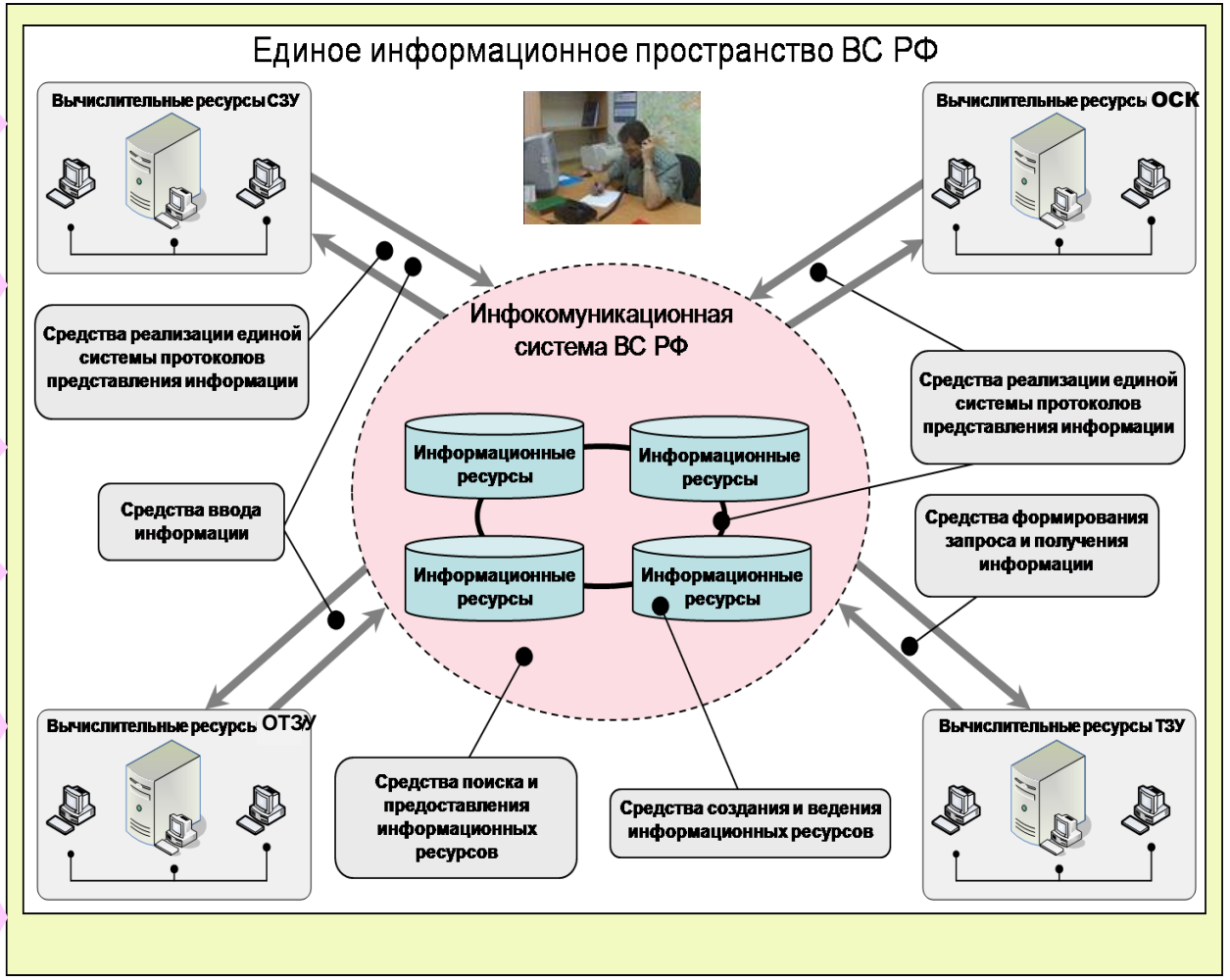
Угрозы:

- контроль Интернет-трафика потенциальным противником и сбор статистики по национальному трафику, сбор статистики по вычислительным ресурсам, оценка уровня их использования для национальной обороны.
- использование вычислительных и частотных ресурсов России для решения военных задач.
- несанкционированное использование противником канальной емкости систем связи при проведении военных операций против России или третьих стран.
- целевое нарушение или изменение трафика, разрушение системы связи страны в критические моменты.
- распространение дезинформации.
- поражение вычислительных центров, центров обработки данных и телекоммуникационных сетей путем применения боевых компьютерных вирусов и других средств.
- разведывательно-диверсионная и военная деятельность с применением роботизированных средств и соединений боевых роботов.

Причины взломов информационных систем:

- Уязвимости архитектуры - 39%
- **Ошибки настройки и управления – 54%**
- Прямой взлом (brute attack) – 4%
- Социальная инженерия – 3%

Информационная инфраструктура системы управления



Угрозы безопасности встроенного программного обеспечения BIOS

Злоумышленник

Технологии удаленного управления

Недокументированные возможности

Официально реализуемые функции технологии удаленного управления
(ASF, WFM, Preboot Execution Environment PXE,IPMI, AMT, DPC, CompuTrace, FailSafe, Remote KVM, Remote Media Redirection, Serial – over-LAN Web Service for Management и т.п.)

-Включение питания, выключение питания, сброс компьютера
-Перенаправление процесса загрузки ОС
-Перенаправление консоли ввода-вывода системы во время процесса загрузки,
-Доступ и удаленная смена установок BIOS.
-Проверка факта запуска критичного ПО на удаленной системе (например, антивирусного агента)
-Восстановление жесткого диска или по сети или с локального образа
-Получение набора ПО на удаленном жестком диске
-Определение и блокирование подозрительного трафика с вирусоподобным или поведением, получаемым или передаваемым удаленной системой.

Последствия:

- непосредственное воздействие на хранимую и обрабатываемую информацию;

- обход модулей защиты, в том числе АПМДЗ;

- перепрограммирование BIOS и модификация исполняемого ПО на НЖМД;

- воздействие на параметры надежности функционирования;

- построение эффективных атак, путем сообщения злоумышленнику информации о текущих параметрах.

Программное обеспечение АС

80% используемого в стране ПО – зарубежного производства

ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Специальное программное обеспечение (СПО)

Функциональные задачи

Общесистемное программное обеспечение (ОСПО)

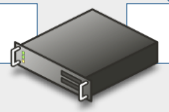
Подкласс управляющих программ

Подкласс прикладных программ

Общее программное обеспечение (ОПО)

Операционные системы

Системы управления базами данных



Доверенная среда

Открытое (свободное) ПО

Интеграция с отечественным проприетарным ПО

Основные цели кибератак на инфраструктуру геопространственных данных

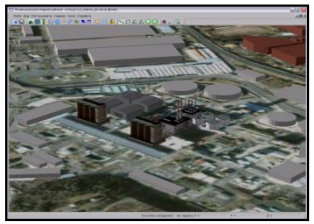
Ухудшение разрешающей способности

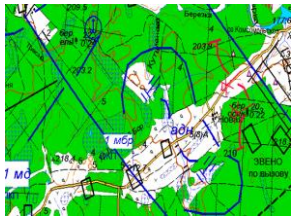
Искажение содержания

Зашумление и геометрические искажения

Искажение навигационных данных

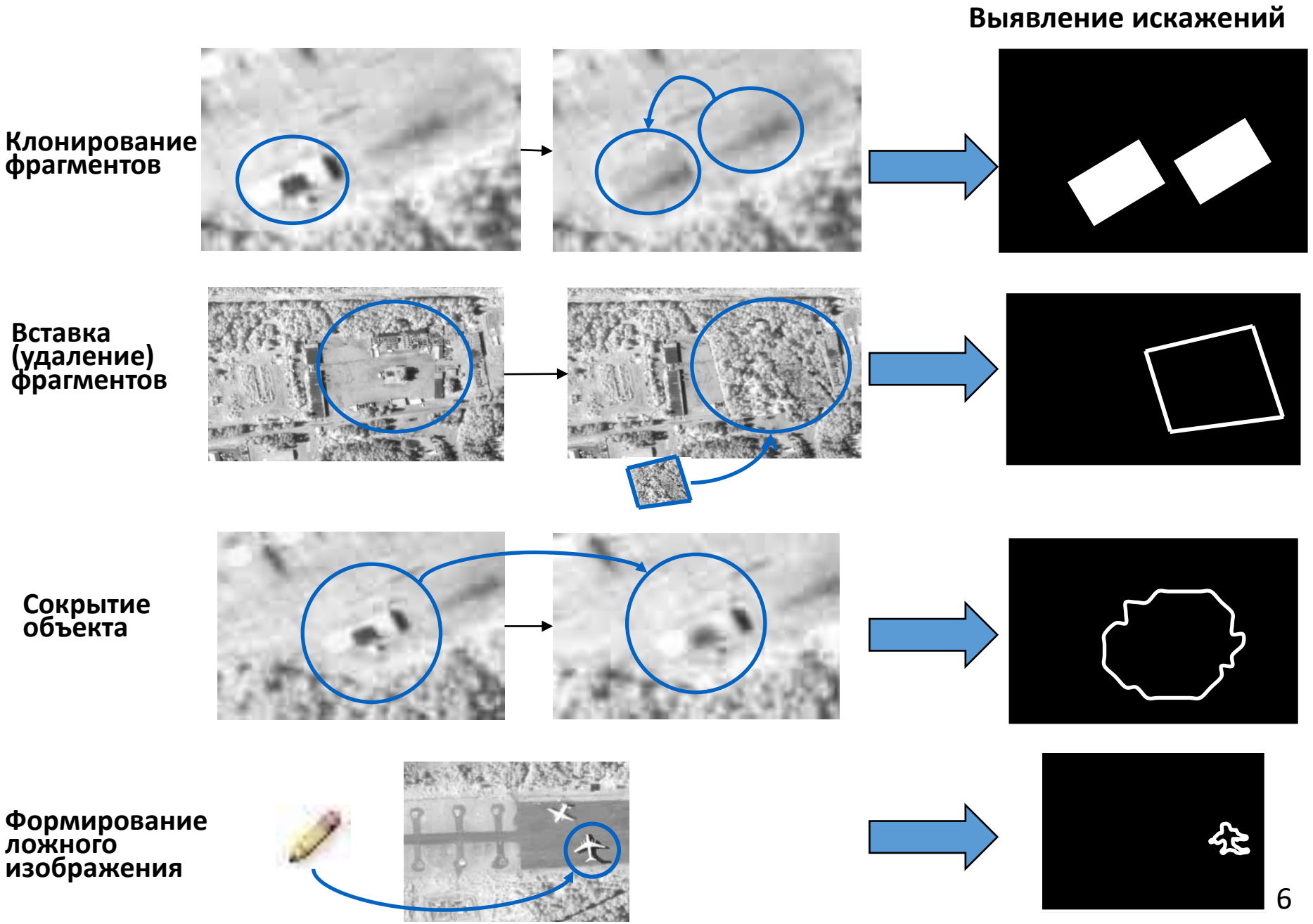
Нарушение достоверности и полноты ГПД



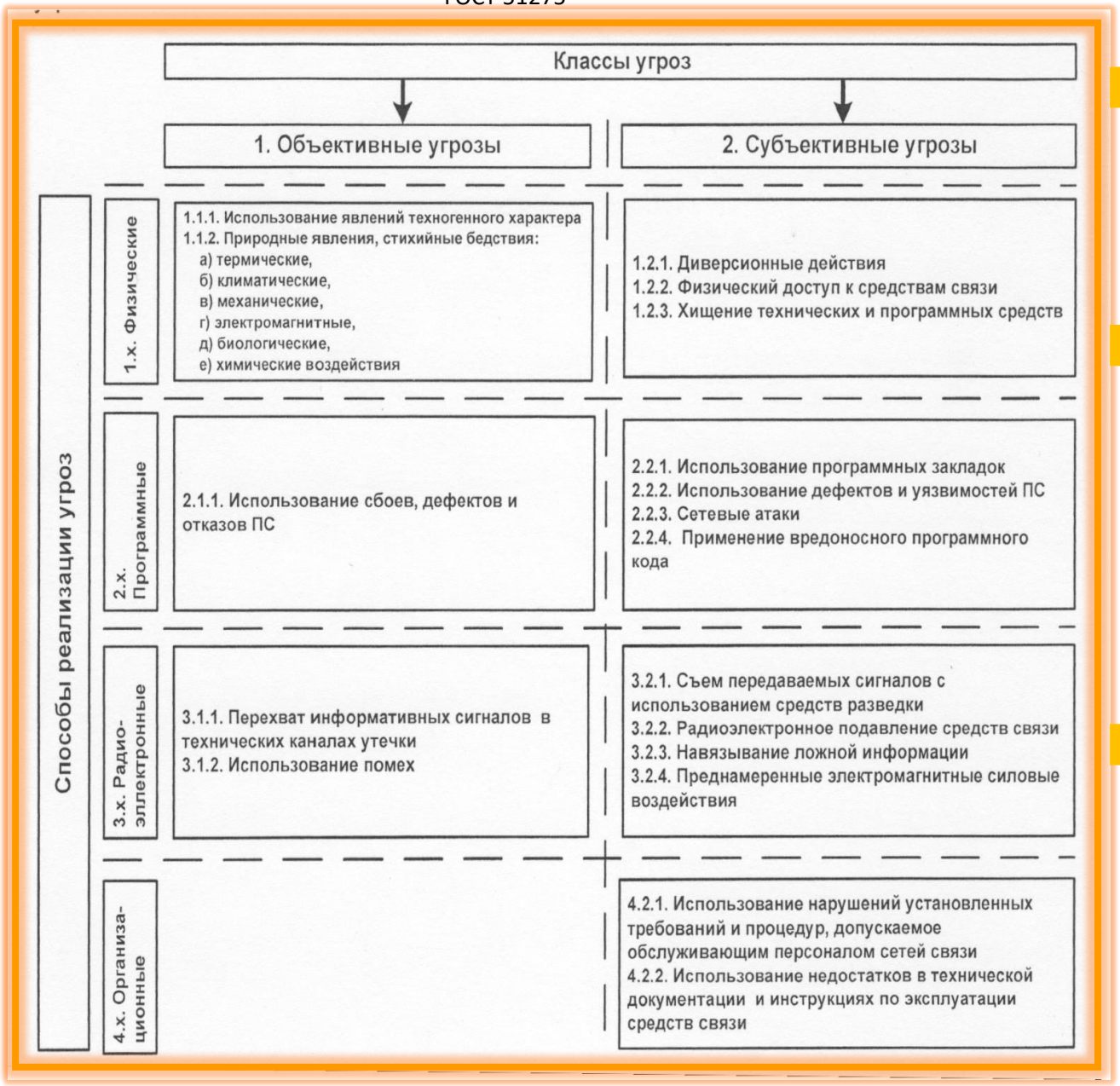


ГИС АС

Типовые атаки «нарушителя»



ГОСТ 51275



- Сервисы
- Системы управления связью
- Сети доступа
- Транспортная сеть

Уровень сетевой инфраструктуры ССОП

- Кража, утечка, потеря;
- Уничтожение, искажение, модификация;
- Отказ в обслуживании;
- НСД;
- Диверсия , ЧС.

Наносимый урон

- безопасности информации, обрабатываемой и передаваемой;
- функционированию средств и систем передачи и обработки данных;
- функционированию систем защиты информации и вычислительной техники;
- персоналу и пользователям ТКС;
- правильности принятия решений;
- нарушения порядка управления ТКС;
- информационному и программному взаимодействию внутри ТКС.

Модель угроз

Модель угроз – это перечень возможных угроз.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.
Итак, **модель угроз** – это документ, тем или иным способом описывающий возможные угрозы безопасности персональных данных.

Зачем нужна модель угроз

Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

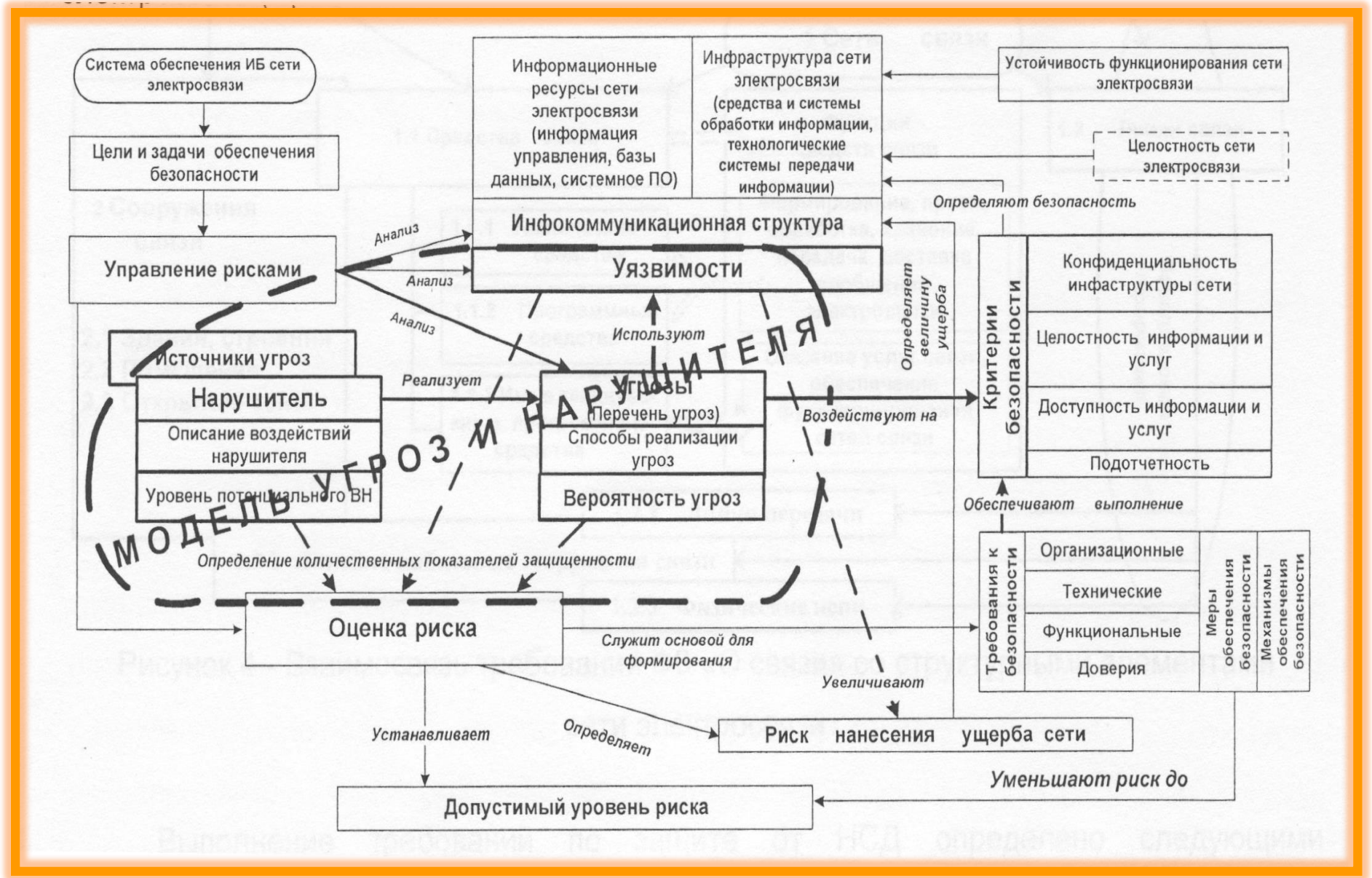
В систему защиты включаются только те средства защиты информации, которые нейтрализуют актуальные угрозы.

Разработка модели угроз безопасности персональных данных

Модель угроз (или как ее еще называют "Частная модель угроз") может разрабатываться ответственными за защиту персональных данных в организации. Также могут привлекаться сторонние эксперты. Разработчики модели угроз должны владеть полной информацией об информационной системе персональных данных, знать нормативную базу по защите информации.

«Базовая модель» содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Многие эксперты по защите информации весьма скептически относятся к этому документу. Угрозы, приведенные в базовой модели, устарели и далеко не всеобъемлющи. Однако за неимением лучшего приходится довольствоваться текущей редакцией документа.

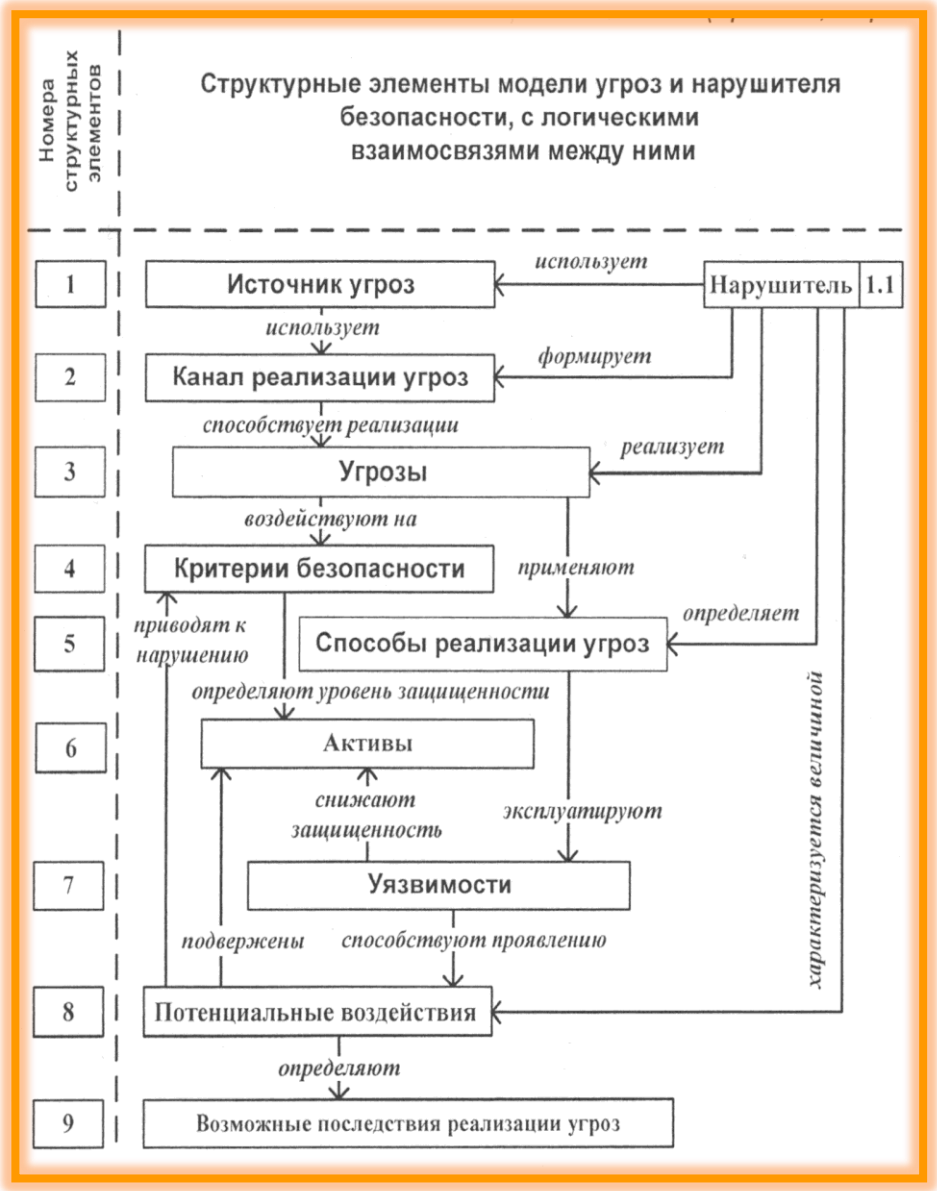
Документ **«Методика определения актуальных угроз»** содержит алгоритм оценки угрозы. Путем несложных расчетов определяется статус каждой вероятной угрозы.


Система обеспечения ИБ сети электросвязи
Цели и задачи обеспечения безопасности
Управление рисками
Информационные ресурсы сети электросвязи (информация управления, базы данных, системное ПО)
Инфраструктура сети электросвязи (средства и системы обработки информации, технологические системы передачи информации)
Инфокоммуникационная структура
Уязвимости
Устойчивость функционирования сети электросвязи
Целостность сети электросвязи
Определяют безопасность
Анализ
Анализ
Анализ
Используют
Определяет величину ущерба
Критерии безопасности
Конфиденциальность инфраструктуры сети
Целостность информации и услуг
Доступность информации и услуг
Подотчетность
Источники угроз
Нарушитель
Описание воздействий нарушителя
Уровень потенциального ВН
Реализует
Угрозы
(Перечень угроз)
Способы реализации угроз
Вероятность угроз
Воздействуют на
МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ
Обеспечивают выполнение
Требования к безопасности
Организационные
Технические
Функциональные
Доверия
Меры обеспечения безопасности
Механизмы обеспечения безопасности
Определение количественных показателей защищенности
Оценка риска
Служит основой для формирования
Увеличивают
Устанавливает
Определяет
Риск нанесения ущерба сети
Уменьшают риск до
Допустимый уровень риска

Структура модели угроз и нарушителя

Внешние нарушители:

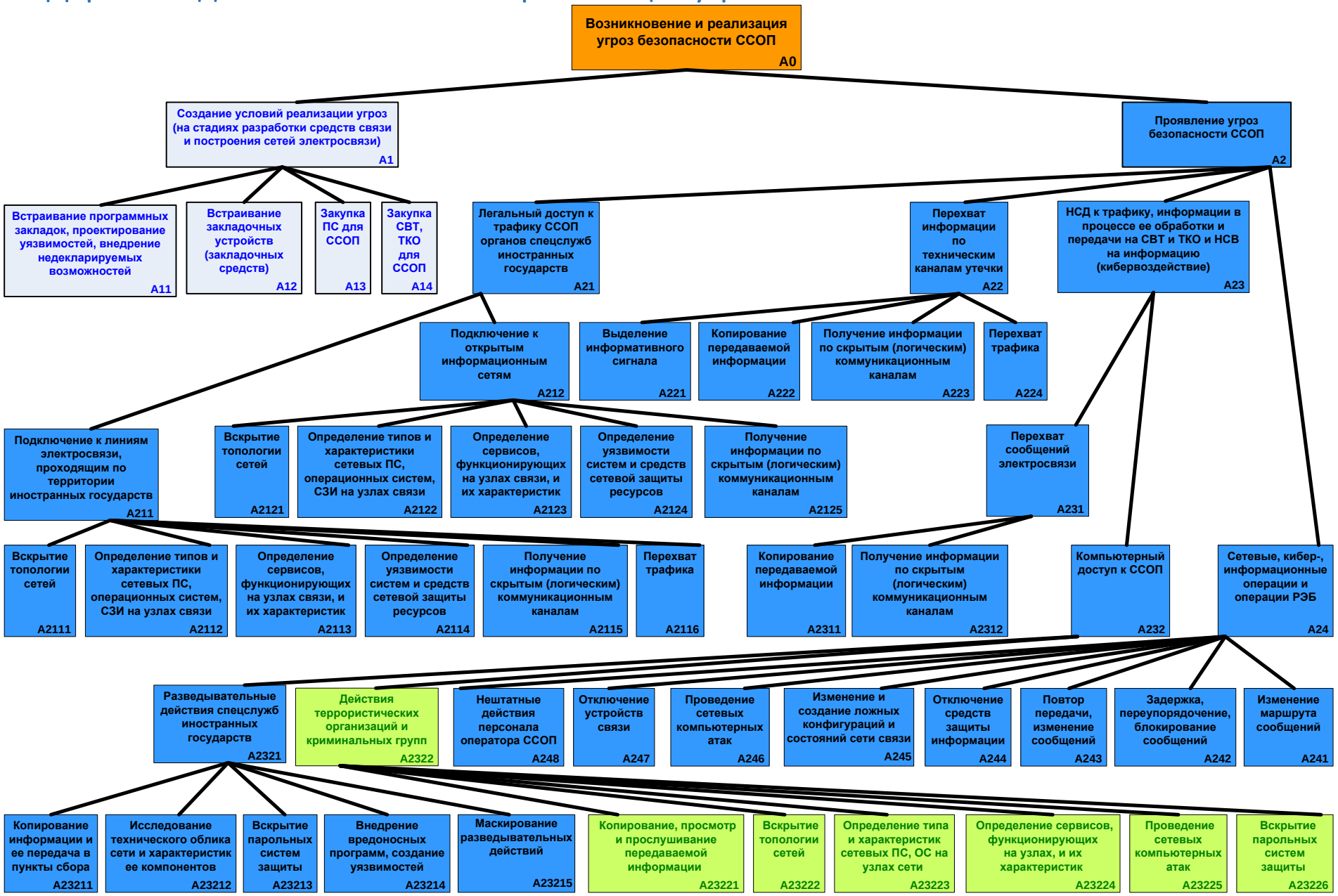
- спецслужбы иностранных государств и блоков государств;
- террористы и террористические организации;
- представители криминальных структур;
- взломщики программных продуктов ИТ, использующихся в сетях и системах связи;
- представители конкурирующих организаций;
- недобросовестные партнеры;
- бывшие сотрудники организаций связи;
- пользователи услугами связи.

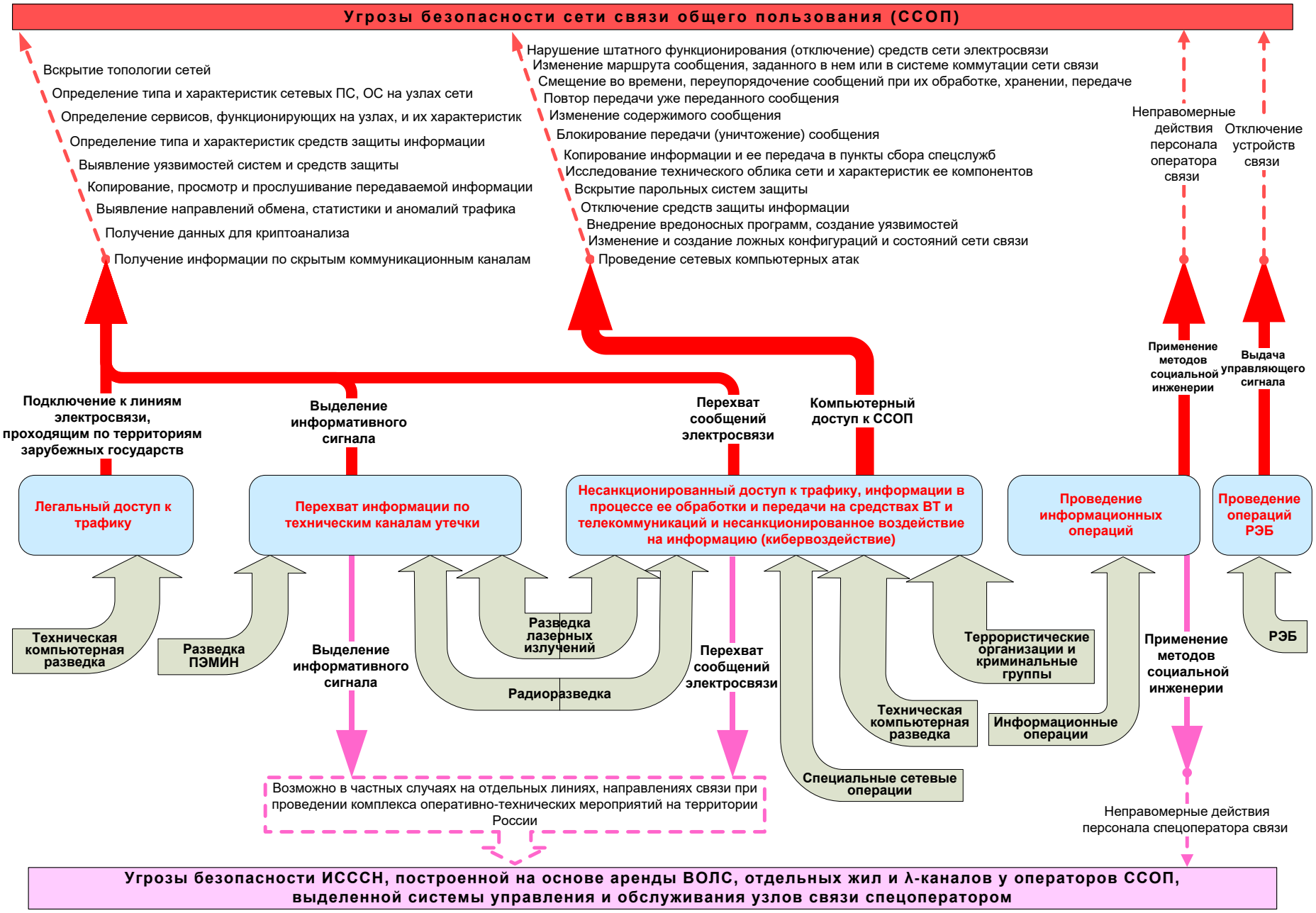


Внутренние нарушители:

- посторонние лица, имеющие санкционированный доступ в КЗ, но не имеющие доступа к инфокоммуникацион-ным ресурсам;
- разработчики средств и систем связи;
- поставщики, в том числе инструментальных средств для разработки;
- изготовители;
- наладчики;
- обслуживающий персонал:
- администраторы, лица, осуществляющие поддержку функционирования средств и систем связи.

Дерево модели возникновения и реализации угроз безопасности



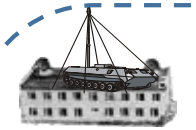

Угрозы безопасности сети связи общего пользования (ССОП)
Вскрытие топологии сетей
Определение типа и характеристик сетевых ПС, ОС на узлах сети
Определение сервисов, функционирующих на узлах, и их характеристик
Определение типа и характеристик средств защиты информации
Выявление уязвимостей систем и средств защиты
Копирование, просмотр и прослушивание передаваемой информации
Выявление направлений обмена, статистики и аномалий трафика
Получение данных для криптоанализа
Получение информации по скрытым коммуникационным каналам
Нарушение штатного функционирования (отключение) средств сети электросвязи
Изменение маршрута сообщения, заданного в нем или в системе коммутации сети связи
Смещение во времени, переупорядочение сообщений при их обработке, хранении, передаче
Повтор передачи уже переданного сообщения
Изменение содержимого сообщения
Блокирование передачи (уничтожение) сообщения
Копирование информации и ее передача в пункты сбора спецслужб
Исследование технического облика сети и характеристик ее компонентов
Вскрытие парольных систем защиты
Отключение средств защиты информации
Внедрение вредоносных программ, создание уязвимостей
Изменение и создание ложных конфигураций и состояний сети связи
Проведение сетевых компьютерных атак
Неправомерные действия персонала оператора связи
Отключение устройств связи
Применение методов социальной инженерии
Выдача управляющего сигнала
Подключение к линиям электросвязи, проходящим по территориям зарубежных государств
Выделение информативного сигнала
Перехват сообщений электросвязи
Компьютерный доступ к ССОП
Легальный доступ к трафику
Перехват информации по техническим каналам утечки
Несанкционированный доступ к трафику, информации в процессе ее обработки и передачи на средствах ВТ и телекоммуникаций и несанкционированное воздействие на информацию (кибервоздействие)
Проведение информационных операций
Проведение операций РЭБ
Техническая компьютерная разведка
Разведка ПЭМИН
Выделение информативного сигнала
Разведка лазерных излучений
Радиоразведка
Перехват сообщений электросвязи
Террористические организации и криминальные группы
Техническая компьютерная разведка
Информационные операции
Специальные сетевые операции
Применение методов социальной инженерии
РЭБ
Возможно в частных случаях на отдельных линиях, направлениях связи при проведении комплекса оперативно-технических мероприятий на территории России
Неправомерные действия персонала спецоператора связи
Угрозы безопасности ИССС, построенной на основе аренды ВОЛС, отдельных жил и λ-каналов у операторов ССОП, выделенной системы управления и обслуживания узлов связи спецоператором

Модель угроз функционированию сетей связи

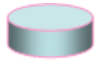
Система мониторинга угроз и реального уровня защищенности сети связи

Угрозы

- Применение оружия, диверсии, катастрофы;
- Хищение технических и программных средств;
- Использование недоверенных СУБД и аппаратных средств;
- Использование недоверенного ПО, программных закладок, вредоносного программного кода, ошибок и дефектов ПО;
- Сетевые и компьютерные атаки (DoS и DDoS - атаки);
- Утечка информации по техническим каналам;
- Радиоэлектронное подавление электромагнитное силовое воздействие;
- Воздействия на парольно-ключевые системы защиты, обработки и передачи информации;
- Ошибки операторов (персонала сетей связи) и преднамеренные вредоносные действия;
- Ошибки и недостатками проектирования и эксплуатации элементов ТКС;
- Использование недостатков технической документации.



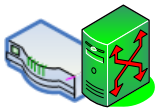
Узлы доступа



БД

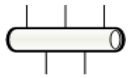
Сервера

ПС



ЦКО

СЗИ



ЛВС

Персонал

Документация

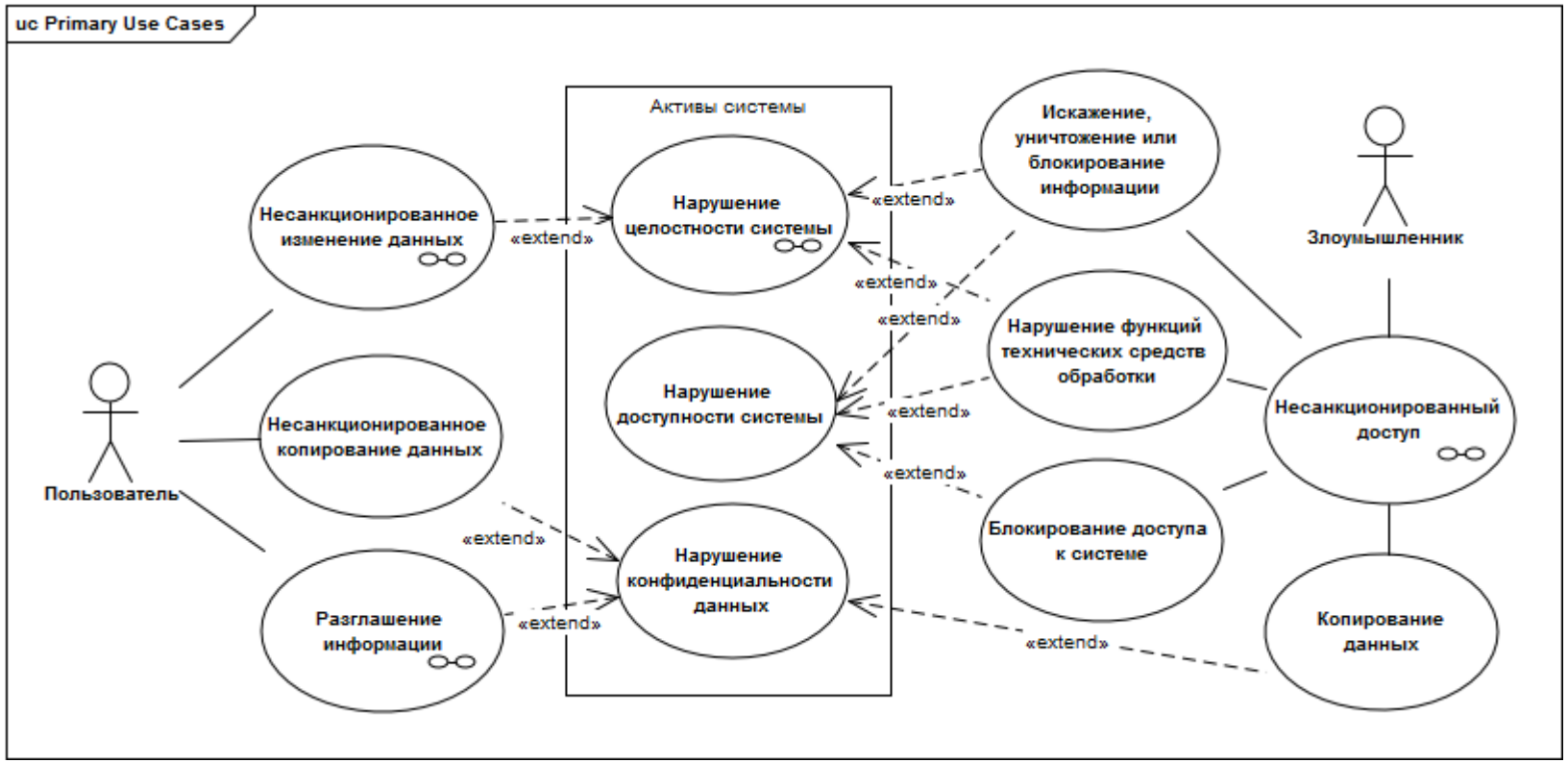
Классификация основных уязвимостей сетей и систем связи:

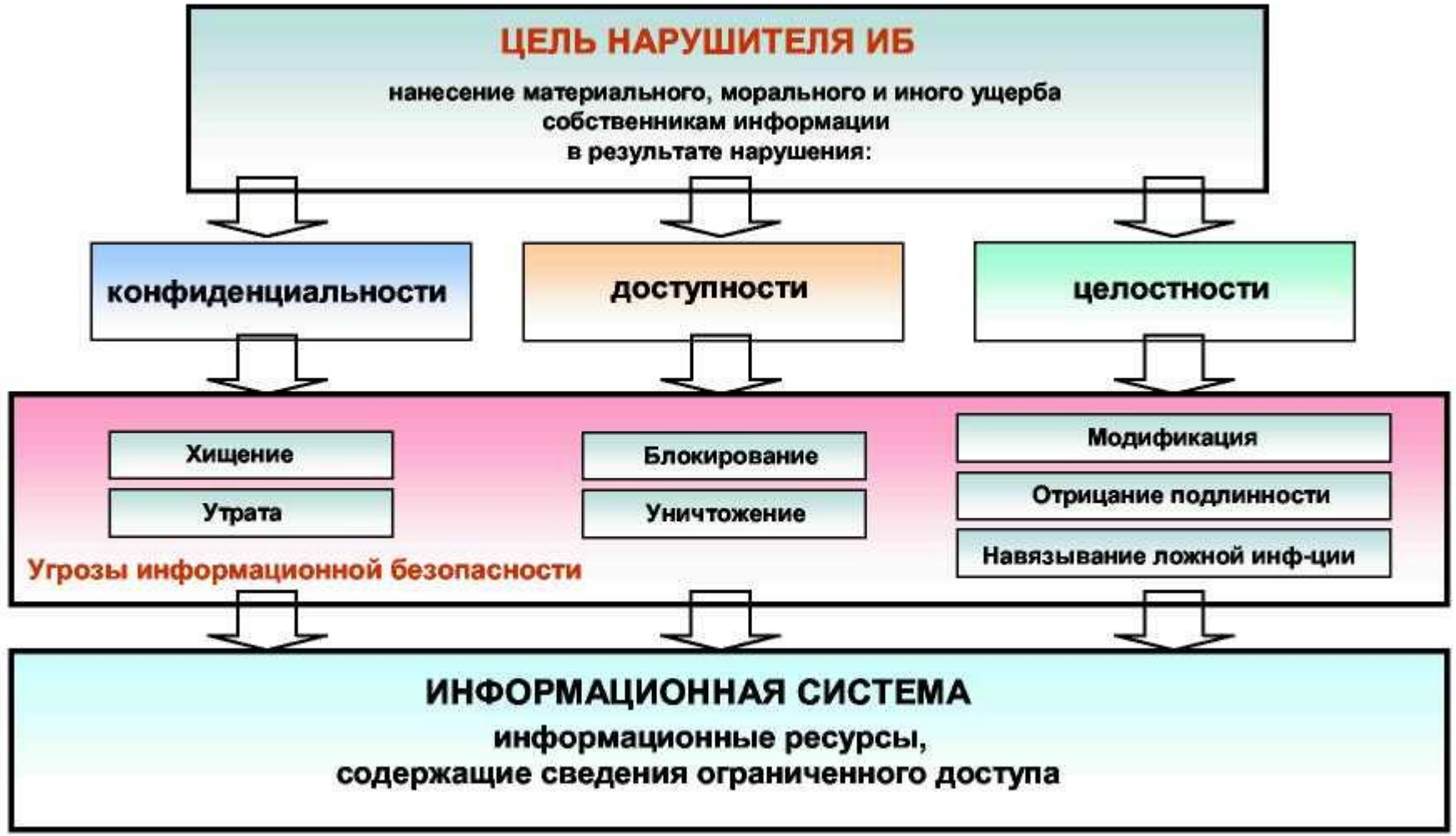
- систем энергоснабжения;
- каналов связи, полей радиообмена, РЭС;
- аппаратных средств;
- системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- прикладного программного обеспечения (в том числе средств защиты информации);
- носителей информации;
- документации;
- персонала.

Проявление

- Несанкционированный доступ к передаваемой информации путем перехвата или перенаправления трафика в целях последующего анализа его информационного содержания;
- Внесение не обнаруживаемой сетью ошибки в информационную или служебную часть сообщения;
- Нарушение необходимого уровня обслуживания или полная блокировка доступа к ресурсу;
- Останов и перезапуск технических средств (нарушение связи);
- Установка несанкционированных режимов технической эксплуатации и видов обслуживания;
- Модификация ПО, путем скрытного добавления новых функций.

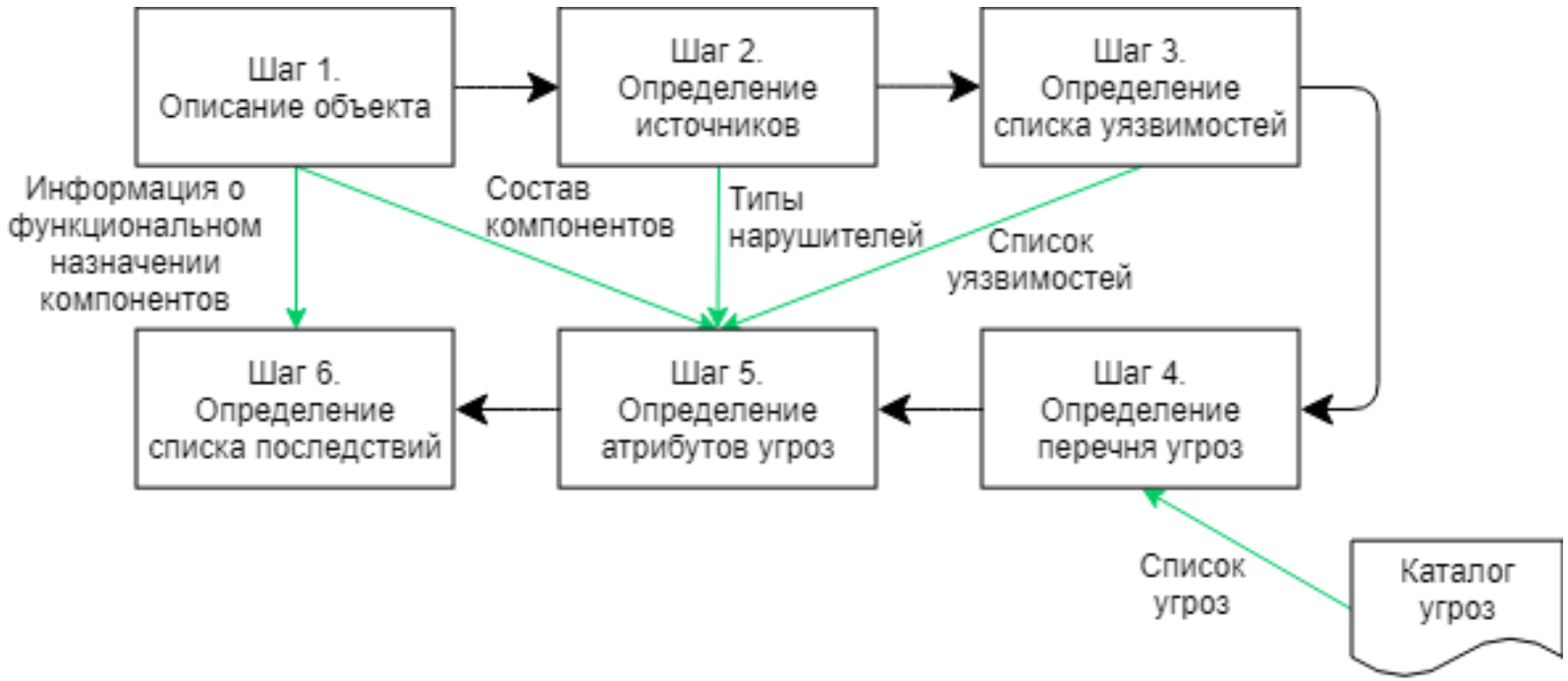
Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, технических и материальных средствах и т.




ЦЕЛЬ НАРУШИТЕЛЯ ИБ
нанесение материального, морального и иного ущерба
собственникам информации
в результате нарушения:
конфиденциальности
доступности
целостности
Хищение
Утрата
Блокирование
Уничтожение
Модификация
Отрицание подлинности
Навязывание ложной инф-ции
Угрозы информационной безопасности
ИНФОРМАЦИОННАЯ СИСТЕМА
информационные ресурсы,
содержащие сведения ограниченного доступа

Моделирование угроз - это итеративный процесс, который состоит из определения активов предприятия, определения того, что каждая информационная система делает с этими активами, создания профиля безопасности для каждой ИС, определения потенциальных угроз, установления приоритетов

Моделирование угроз



Вопросы для прикрепления материала:

1. Были ли в вашей практике случаи попыток реализации программных (компьютерных) атак на информацию, обрабатываемую в АС? Охарактеризуйте последствия программного воздействия, проявившиеся в каждом конкретном случае и оцените возможную уязвимость информации.

2. Какие вам известны подходы к классификации угроз кибербезопасности? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте таксономию угроз кибербезопасности АС.

4. Рассмотрите возможности несанкционированного получения информации в рассматриваемой АС, когда возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС.

5. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

6. Каковы основные способы проведения информационных операций?

7. Охарактеризуйте типологию киберпреступлений. В чем отличие и сходство деструктивного информационного воздействия со стороны кибертеррористов, хакеров?

Спасибо за внимание!