Приложение 1

Требования к классам защищенности и к автоматизированной системе

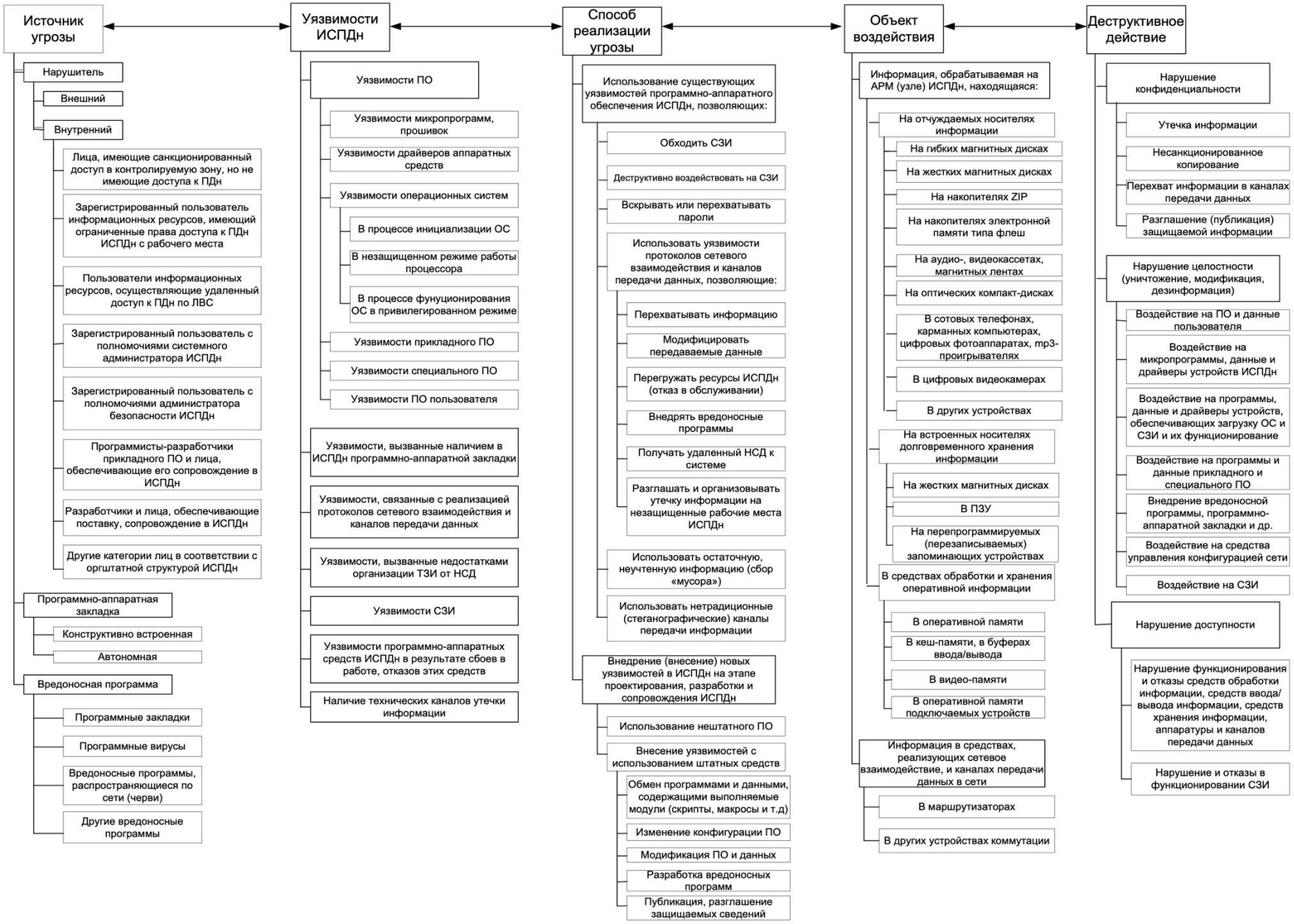
Подсистемы и требования	Классы			АС
	1В	1Г	1Д	
1. Подсистема управления доступом				
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:				
в систему	+	+	+	+
к терминалам, электронно-вычислительным машинам (ЭВМ), узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	+	+	-	+
к программам	+	+	-	+
к томам, каталогам, файлам, записям, полям записей	+	+	-	+
1.2. Управление потоками информации	+	-	-	+
2. Подсистема регистрации и учета				
2.1. Регистрация и учет:				
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+
выдачи печатных (графических) выходных документов	+	+	-	+
запуска (завершения) программ и процессов (заданий, задач)	+	+	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	+	+	-	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	+	+	-	+
изменения полномочий субъектов доступа	+	-	-	+
создаваемых защищаемых объектов доступа	+	-	-	+
2.2. Учет носителей информации	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+	+	-	+
2.4. Сигнализация попыток нарушения защиты	+	-	-	+
3. Криптографическая подсистема	+	+	+	+
4. Подсистема обеспечения целостности				
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	+	-	-	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+
4.6. Использование сертифицированных средств защиты	+	-	-	+

Обозначения:

" - " - нет требований к данному классу;

" + " - есть требования к данному классу.

Элементы описания угроз НСД к информации в ИСПДн



Классификация уязвимостей программного обеспечения

Приложение 4

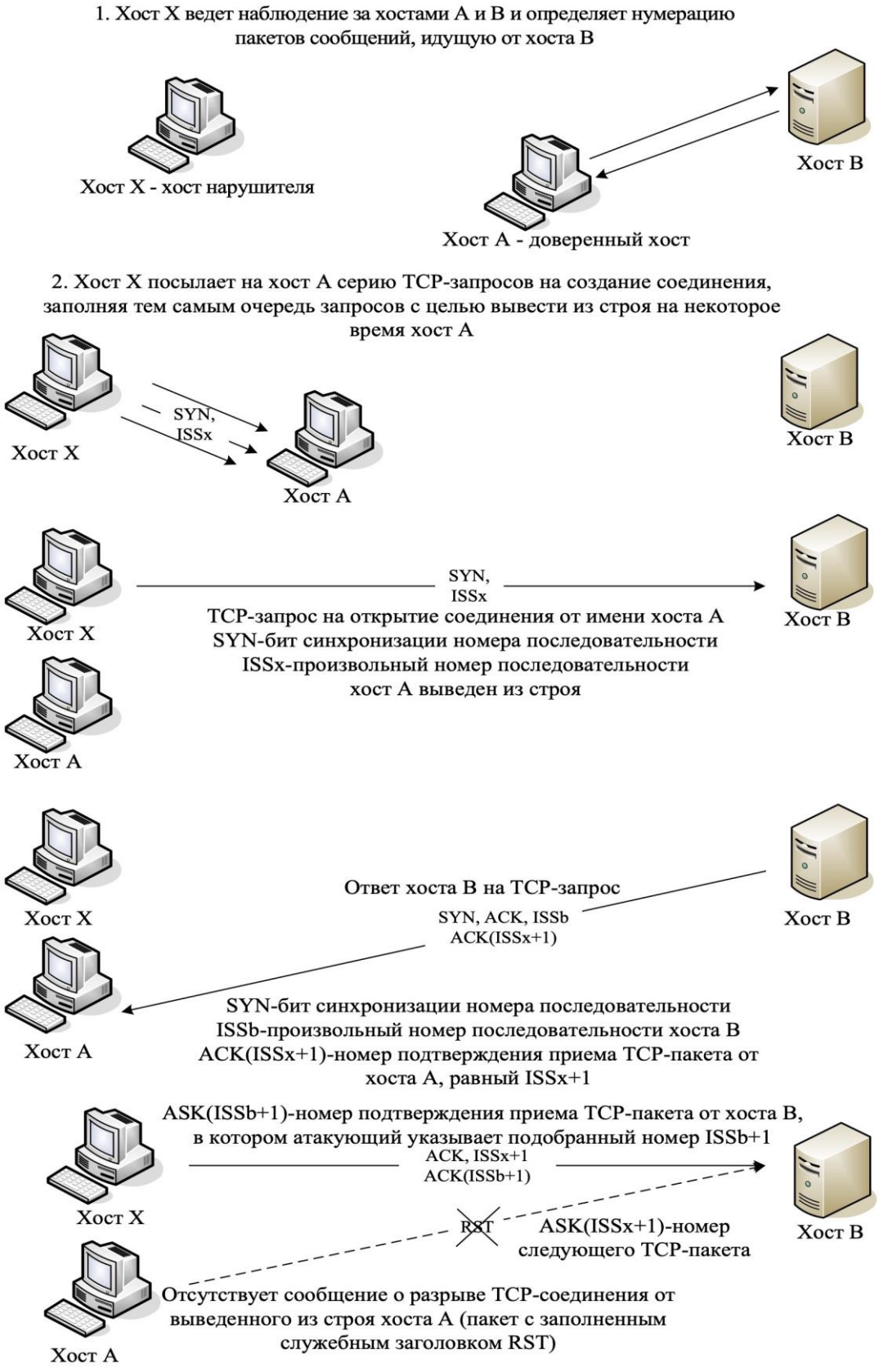
Уязвимости отдельных протоколов стека протоколов TCP/IP,
на базе которого функционируют глобальные сети общего пользования

Наименование протокола	Уровень стека протоколов	Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
FTP (File Transfer Protocol) – протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) 2. Доступ по умолчанию 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам
telnet – протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам
UDP – протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера	Возможность реализации UDP-шторма. В результате обмена пакетами происходит существенное снижение производительности сервера
ARP – протокол преобразования IP-адреса в физический адрес	Сетевой	Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде)	Возможность перехвата трафика пользователя злоумышленником
RIP – протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута	Возможность перенаправления трафика через хост злоумышленника
TCP – протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP
Наименование протокола	Уровень стека протоколов	Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
DNS – протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	Фальсификация ответа DNS-сервера
IGMP – протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Зависание систем Win 9x/NT/200
SMTP – протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения
SNMP – протокол управления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность переполнения пропускной способности сети

Схема реализации угрозы «Анализ сетевого трафика»

Приложение 6

Схема реализации угрозы «Подмена доверенного объекта сети»



Приложение 7

Возможные последствия реализации угроз различных классов

№ п/п	Тип атаки		Возможные последствия
1	Анализ сетевого трафика		Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2	Сканирование сети		Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3	«Парольная» атака		Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа
4	Подмена доверенного объекта сети		Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
5	Навязывание ложного маршрута		Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6	Внедрение ложного объекта сети		Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
7	Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств

№ п/п	Тип атаки		Возможные последствия
8	Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Классификация программных вирусов и сетевых червей