ДиалогНаука

Практические аспекты выполнения требований законодательства в области защиты персональных данных

Виктор Сердюк, к.т.н., CISSP

Генеральный директор
ЗАО «ДиалогНаука»

О компании «ДиалогНаука»

- Создано в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были ревизор ADinf, Doctor Web и Aidstest
- В настоящее время ДиалогНаука является системным интегратором в области информационной безопасности

ДиалОгНаука

ФЗ «О персональных данных»

- Федеральный закон «О персональных данных» № 152-ФЗ был принят Государственной думой 08.07.2006 и одобрен Советом Федерации 14.07.2006
- Федеральный закон полностью вступил в силу с 01.07.2011
- Федеральным законом регулируются отношения, связанные с обработкой персональных данных
- Целью Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну

ДиалогНаука

Ключевые изменения терминологии

Изменения терминов	Примечания
Персональные данные - любая информация, относящаяся к определенному или определяемому ~~на основании такой информации~~ физическому лицу (субъекту персональных данных)~~, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация~~	Понятие стало более размытым
Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных	Расширен перечень действий с ПДн
Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники	Новый термин, исключает «неавтоматизированную обработку» ПДн в электронном виде
Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц	Новый термин, фактически означает отнесение ПДн к общедоступным

ДиалогНаука

Ключевые изменения терминологии

Изменения терминов	Примечания
Предоставление персональных данных - действия, направленные на раскрытие персональных данных **определенному лицу** или **определенному кругу** лиц	Понятие стало более конкретным
Блокирование персональных данных - временное прекращение **обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)**	Распространяется на все действия с ПДн, предусматривается возможность уточнения заблокированных ПДн
Уничтожение персональных данных - действия, в результате которых **становится невозможным** восстановить содержание персональных данных в информационной системе персональных данных **и (или)** в результате которых уничтожаются материальные носители персональных данных	Небольшое уточнение
Обезличивание персональных данных - действия, в результате которых **становится невозможным без использования дополнительной информации** определить принадлежность персональных данных конкретному субъекту персональных данных	Важное уточнение, стало больше основания для отнесения к обезличенным ПДн

ДиалогНаука

Ключевые изменения терминологии

Изменения терминов	Примечания
Информационная система персональных данных - совокупность **содержащихся в базах данных** персональных данных и **обеспечивающих их обработку информационных технологий** и технических средств	Понятие стало более конкретным, исключило обработку ПДн без использования средств автоматизации в ИСПДн
Трансграничная передача персональных данных - передача персональных данных **на территорию иностранного государства** органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу	Исчезло непонятное «через границу РФ», понятие стало более корректным

Удалены понятия	
Использование ПДн	Термин, пересекающийся с обработкой
Конфиденциальность ПДн	Избыточный термин с учетом введения терминов «распространение», «предоставление» и др.
Общедоступные ПДн	Избыточный термин с учетом введения терминов «распространение», «обезличивание» и др.

Отраслевые стандарты

На основании и во исполнение федеральных законов государственные органы, ***Банк России, органы местного самоуправления*** в пределах своих полномочий могут принимать ***нормативные правовые акты, нормативные акты, правовые акты (далее нормативные правовые акты)*** по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, ***устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности***, и подлежат официальному опубликованию.

ДиалогНаука

Новые требования по защите ПДн

Оператор самостоятельно определяет состав и перечень мер необходимых и достаточных для выполнения требований Закона, в том числе:

- **назначает ответственного за организацию обработки** персональных данных
- **принимает внутренние нормативные документы** по вопросам обработки и защиты персональных данных
- принимает **правовые, организационные и технические меры** защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий
- **осуществляет внутренний контроль** за соответствием обработки персональных данных Закону
- **осуществляет оценку вреда субъектам** при нарушении Закона и соотношения вреда и применяемых мер в соответствии с Законом
- **ознакамливает работников** с положениями законодательства и внутренними требованиями по вопросам обработки персональных данных
- обеспечивает неограниченный доступ к политике в области персональных данных

ДиалогНаука

Новые требования по защите ПДн

Обеспечение безопасности персональных данных достигается:

- определением угроз
- применением организационных и технических мер, обеспечивающих установленные Правительством РФ уровни защищенности персональных данных
- применением **СЗИ прошедших оценку соответствия**
- оценкой эффективности мер по обеспечению безопасности персональных данных **до ввода эксплуатацию ИСПДн**
- учетом носителей персональных данных
- обнаружением фактов НСД к персональных данных и принятием мер
- восстановлением персональных данных установлением правил доступа к персональных данных
- регистрации всех действий с персональных данных
- контролем за принимаемыми мерами

Лицо, ответственное за организацию обработки персональных данных

Лицо, ответственное за организацию обработки персональных данных:

- подотчетно исполнительному органу оператора
- осуществляет внутренний контроль за соблюдением требований законодательства
- доводит до сведения работников оператора положения законодательства
- организует прием и обработку обращений и запросов субъектов персональных данных

ДиалОгНаука

Согласие на обработку ПДн

- Письменное согласие необходимо только для обработки:
  - биометрических ПДн
  - специальных категорий персональных данных (касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни)
- Согласие на обработку дается в любой форме позволяющей подтвердить факт его получения
- Обработчик ПДн не должен иметь согласия на обработку, его должен иметь оператор. Обработчик производит обработку ПДн на основании поручения оператора.
- Обязанность предоставлять согласия возложена на оператора ПДн

ДиалОгНаука

Ответственность

- Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность
- Меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований ФЗ «О персональных данных»
- Направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн
- Приостановка действия или лишение лицензий, без которых деятельность по обработке персональных данных становится незаконной.

ДиалОгНаука

Ответственность

- Изъятие несертифицированных средств защиты информации (в т.ч. основного оборудования и программного обеспечения ИС, т.к. персональные данные обрабатываются непосредственно в ИС, а средства защиты интегрированы в стандартное оборудование и программное обеспечение ИС)
- Изъятие используемых средств шифрования
- Привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей уголовного и административного кодекса

ДиалОгНаука

Требования ФЗ «О персональных данных»

Статья 21. Пункт 3. В случае выявления ***неправомерной обработки*** персональных данных, ***осуществляемой оператором или лицом, действующим по поручению оператора,*** оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан ***прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора***. В случае ***если обеспечить правомерность обработки персональных данных невозможно***, оператор в срок, не превышающий ***десяти*** рабочих дней с даты выявления ***неправомерной обработки*** персональных данных, обязан уничтожить такие персональные данные ***или обеспечить их уничтожение***. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение *субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных* были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

ДиалОгНаука

Новые требования по защите ПДн

- Правительство РФ с учетом ущерба субъекту, типа персональных данных, вида деятельности устанавливает:
  - **уровни защищенности** персональных данных
  - **требования, выполнение которых обеспечит достижение заданного уровня защищенности** персональных данных
  - требования к носителям биометрических данных

ФЗ «О персональных данных»

Информационные системы персональных данных, созданные до 1 января 2011 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона **не позднее 1 июля 2011 года**

ДиалОгНаука

Документы, разработанные на основе ФЗ «О персональных данных»

- Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн"
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации
- Приказ ФСТЭК, ФСБ, Мининформсвязи от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации ИСПДн»

ДиалОгНаука

Документы ФСТЭК

- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в ИСПДн (**не действует**)
- Рекомендации по обеспечению безопасности персональных данных при их обработке в ИСПДн (**не действует**)
- Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн
- Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн
- Приказ ФСТЭК от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в ИСПДн»

Документы ФСБ

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

ДиалОгНаука

Информационные системы, обрабатывающие персональные данные

- Бухгалтерские программы
- Программы кадрового учета
- CRM-системы с информацией о действующих и потенциальных клиентах
- Системы билинга
- Информационные системы медицинских учреждений
- ERP-системы, обрабатывающие персональные данные
- и др.

ДиалогНаука

Стадии создания системы защиты персональных данных

- подготовительный этап выполнения работ;
- предпроектная стадия, включающая предпроектное обследование ИСПДн, классификацию ИСПДн, а также разработку модели угроз и нарушителя;
- этап разработки комплекта организационно-распорядительных документов;
- стадия проектирования СЗПДн, включающая в себя разработку технического проекта;
- этап ввода в действие СЗПДн;
- оценка соответствия ИСПДн требованиям безопасности информации.

ДиалогНаука

Участники проекта

- **Подразделение информационной безопасности**
  - Согласование документов и процессов, связанных с защитой информации
- **Подразделение информационных технологий**
  - Согласование документов и процессов, связанных с автоматизацией и прикладными системами
- **Подразделение кадровой службы**
  - Согласование документов и процессов, связанных с обработкой ПДн сотрудников компании
- **Подразделение юридической службы**
  - Согласование ОРД
- **Бизнес-подразделения компании**

ДиалОгНаука

Подготовительный этап выполнения работ

- Разработка и утверждение плана выполнения работ
- Назначение ответственных лиц за решение задач в рамках проекта
- Определение варианта выполнения работ по защите персональных данных:
  - Выполнение работ собственными силами;
  - Выполнение работ силами внешнего консультанта;
  - Выполнение работ с привлечение внешнего консультанта

ДиалогНаука

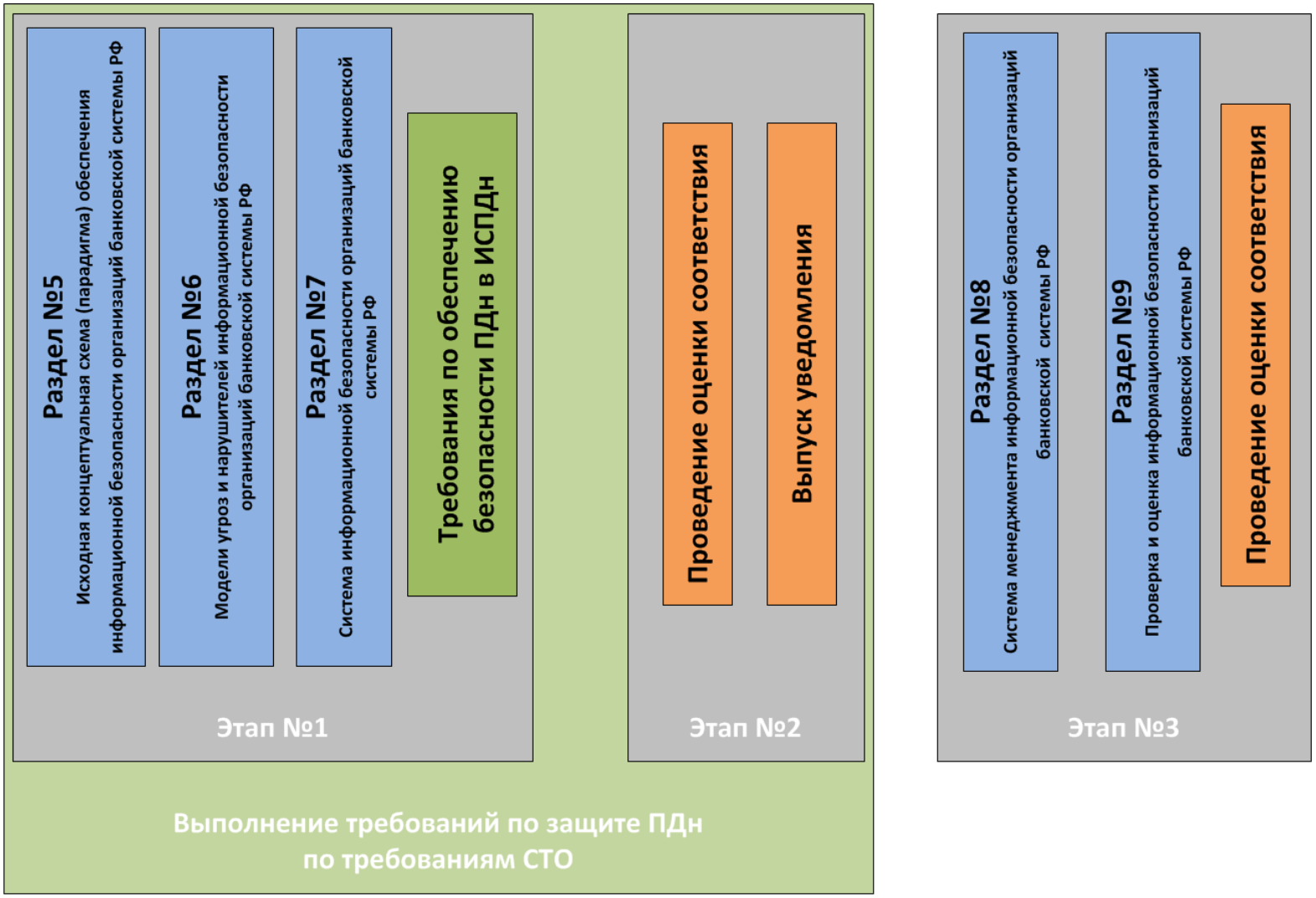
Этапы проведения работ

Работы по защите ПДн в рамках СТО БР ИББС:

- Построение системы обеспечения информационной безопасности персональных данных
- Проведение оценки соответствия и уведомление регуляторов
- Построение системы менеджмента информационной безопасности

ДиалОгНаука

Этапы проведения работ



ДиалОгНаука

Предпроектная стадия

- Анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн
- Определение используемых средств защиты ПДн, и оценка их соответствия требованиям нормативных документов РФ
- Определение перечня ПДн, подлежащих защите
- Определение перечня ИСПДн, обрабатывающих ПДн
- Определение класса ИСПДн;
- Разработка модели нарушителя;
- Разработка частной модели угроз информационной безопасности ПДн.

ДиалОгНаука

Предпроектная стадия

Результаты этапа:

- Отчет о проведенном обследовании, содержащий оценку текущего уровня соответствия требованиям законодательства и детальные рекомендации по устранению выявленных недостатков
- Проекты актов классификации
- Модель угроз безопасности
- Модель нарушителя

Длительность этапа: 1-1,5 месяца

ДиалОгНаука

Предпроектная стадия

Консультант:

- Предоставление опросных листов для сбора исходной информации
- Анализ и уточнение предоставленной информации
- Разработка отчетных материалов по этапу

Заказчик:

- Сбор исходных данных в соответствии с опросными листами Консультанта
- Согласование отчетных материалов

ДиалогНаука

Инструментальный анализ защищенности

- Анализ средств защиты информации
  - Анализ VPN-шлюзов
  - Анализ антивирусных средств защиты
  - Анализ систем обнаружения атак IDS/IPS
  - Анализ межсетевых экранов
  - Анализ систем защиты от утечки конфиденциальной информации
- Анализ безопасности сетевой инфраструктуры
  - Анализ безопасности коммутаторов
  - Анализ безопасности маршрутизаторов
  - Анализ безопасности SAN-сетей
  - Анализ безопасности сетей WLAN

ДиалогНаука

Инструментальный анализ защищенности

- Анализ безопасности общесистемного программного обеспечения
  - Анализ ОС Windows
  - Анализ ОС UNIX
  - Анализ ОС Novell Netware
- Анализ безопасности прикладного программного обеспечения
  - Анализ безопасности баз данных
  - Анализ безопасности почтовых серверов
  - Анализ безопасности Web-серверов
  - Анализ безопасности Web-приложений

ДиалогНаука

Тест на проникновение (Penetration testing)

Тест на проникновение позволяет получить независимую оценку безопасности ИСПДн по отношению к внешнему нарушителю

Исходные данные

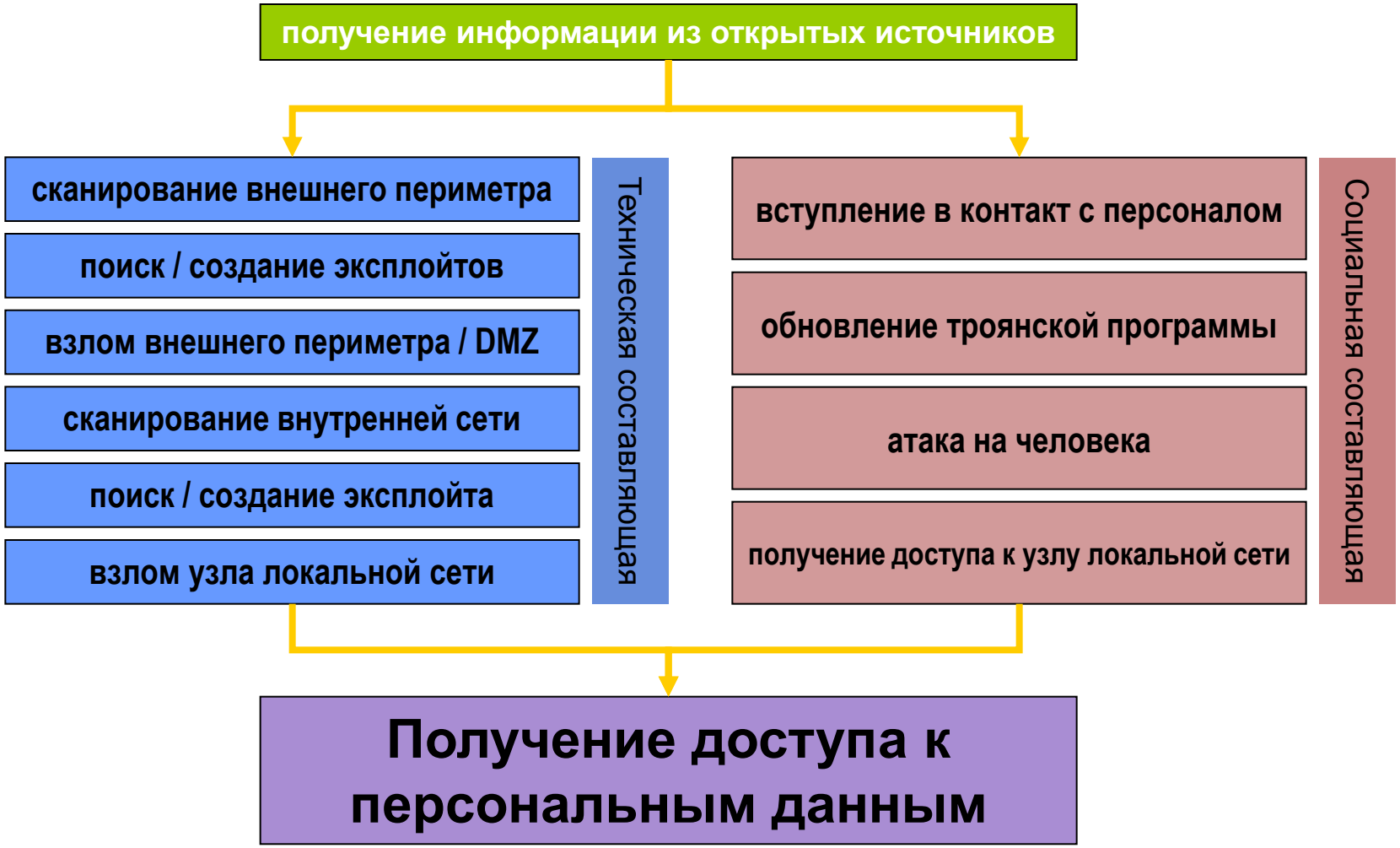
- IP-адреса внешних серверов
- Анализ проводится с внешнего периметра

Собираемая информация

- Топология сети
- Используемые ОС и версии ПО
- Запущенные сервисы
- Открытые порты, конфигурация и т.д.

ДиалогНаука

Обобщенный план теста на проникновение



ДиалОгНаука

Разработка ОРД

- сбор существующей нормативной документации Заказчика описывающей состав, структуру и функциональные возможности, технические характеристики и организацию использования ИСПДн и средств защиты ИСПДн, а так же регламентирующие порядок их взаимодействия
- анализ существующей нормативной документации Заказчика в области обработки и защиты ПДн на предмет соответствия требованием нормативных документов РФ
- Разработка комплекта организационно-распорядительной документации по защите ПДн

ДиалогНаука

Организационно-распорядительная документация

Название	Содержание
Приказ «О создании рабочей группы по приведению информационных систем персональных данных в соответствие с требованиями Федерального Закона «О персональных данных»	Назначает рабочую группу по организации работ по обеспечению безопасности персональных данных, ее обязанности, полномочия, сроки.
	Приложение 1. Состав рабочей группы
	Приложение 2. План мероприятий по защите персональных данных
Приказ «О создании комиссии по классификации информационных систем персональных данных»	Назначает Комиссию по классификации информационных систем персональных данных, ее обязанности, полномочия, сроки.
	Приложение 1. Состав Комиссии
Приказ «Об утверждении актов классификации информационных систем персональных данных»	Утверждает и вводит в действие акты классификации информационных систем персональных данных.
	Приложения: Акты классификации
Приказ «Об утверждении частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных»	Утверждает и вводит в действие «Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
	Приложение 1. «Частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
	Приложение 2[1]. «Модель нарушителя».
Приказ «О введении в действие перечня обрабатываемых персональных данных, перечня информационных систем персональных данных и перечня подразделений и сотрудников, допущенных к работе с персональными данными».	Утверждает и вводит в действие Перечень обрабатываемых персональных данных, Перечень информационных систем персональных данных, Перечень подразделений и должностей, допущенных к работе с персональными данными, Дополнения в Перечень конфиденциальной информации, а так же определяет ответственность должностных лиц.
	Приложение 1. Перечень обрабатываемых персональных данных.
	Приложение 2. Перечень информационных систем персональных данных.
	Приложение 3. Перечень подразделений и должностей, допущенных к работе с персональными данными.
	Приложение 4. Дополнения в Перечень конфиденциальной информации.
Приказ «Об организации работ по обеспечению безопасности персональных данных»	Утверждает и вводит в действие внутренние документы по организации работ и обеспечению безопасности персональных данных.
	Приложение 1 к Приказу. Положение об обработке персональных данных.

Название	Содержание
	Приложение 3 к Положению об обработке персональных данных. Форма Согласия на обработку персональных данных.
	Приложение 4 к Положению об обработке персональных данных. Форма Согласия на внесение персональных данных в общедоступные источники.
	Приложение 5 к Положению об обработке персональных данных. Форма Согласия на получение персональных данных у третьих лиц.
	Приложение 6 к Положению об обработке персональных данных. Форма Отзыва согласия на обработку персональных данных.
	Приложение 7 к Положению об обработке персональных данных. Форма Запроса субъекта персональных данных об обрабатываемых персональных данных.
	Приложение 8 к Положению об обработке персональных данных. Форма Ответа субъекту персональных данных об обрабатываемых персональных данных.
	Приложение 9 к Положению об обработке персональных данных. Форма Запроса субъекта персональных данных об исключении из обработки или исправлении неверных персональных данных, а также данных, обработанных с нарушением требований законодательства.
	Приложение 10 к Положению об обработке персональных данных. Форма Ответа субъекту персональных данных об исключении из обработки или исправлении неверных персональных данных, а также данных, обработанных с нарушением требований законодательства.
	Приложение 11 к Положению об обработке персональных данных. Форма Уведомления субъекта персональных данных о начале обработки персональных данных.
	Приложение 12 к Положению об обработке персональных данных. Форма Запроса третьих лиц на доступ к обрабатываемым персональным данным.
	Приложение 13 к Положению об обработке персональных данных. Форма Ответа на запрос третьих лиц на доступ к обрабатываемым персональным данным.
	Приложение 14 к Положению об обработке персональных данных. Форма Журнала учета обращений субъектов персональных данных.
	Приложение 15 к Положению об обработке персональных данных. Форма Журнала учета выдачи материальных носителей персональных данных.
	Приложение 16 к Положению об обработке персональных данных. Форма Журнала учета материальных носителей персональных данных.
	Приложение 17 к Положению об обработке персональных данных. Форма Акта уничтожения персональных данных.
	Приложение 18 к Положению об обработке персональных данных. Форма журнала учета проверок, проводимых органами государственного контроля (надзора), органами муниципального контроля.
	Приложение 19 к Положению об обработке персональных данных. Форма Соглашения о

Организационно-распорядительная документация

Название	Содержание
	конфиденциальности при передаче персональных данных третьим лицам.
	Приложение 2 к Приказу. Положение об организации и обеспечении защиты персональных данных.
	Приложение 3 к Положению об организации и обеспечении защиты персональных данных. Форма журнала учета средств защиты информации, эксплуатационной и технической документации к ним.
	Приложение 4 к Положению об организации и обеспечении защиты персональных данных. Форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.
	Приложение 5 к Положению об организации и обеспечении защиты персональных данных. Форма журнала периодического тестирования средств защиты информации.
	Приложение 6 к Положению об организации и обеспечении защиты персональных данных. Форма журнала учета мероприятий по защите информации в ИСПДн.
	Приложение 7 к Положению об организации и обеспечении защиты персональных данных. Форма Заявки на предоставление доступа к информационным системам персональных данных.
	Приложение 8 к Положению об организации и обеспечении защиты персональных данных. Форма плана внутренних проверок состояния защиты персональных данных в ИСПДн.
	Приложение 3 к Приказу. Положение об отделе информационной безопасности.
	Приложение 4 к Приказу. Дополнения разделы трудовых договоров о конфиденциальности.
	Приложение 5 к Приказу. Дополнения в должностные инструкции лиц участвующих в обработке персональных данных.
	Приложение 6 к Приказу. Инструкции пользователям информационных систем персональных данных.
	Приложение 7 к Приказу. Инструкции администраторам безопасности информационных систем персональных данных.
	Приложение 8 к Приказу. План внутренних проверок состояния защиты персональных данных в ИСПДн.
	Приложение 9 к Приказу. Перечень мест хранения материальных носителей персональных данных.

ДиалогНаука

Организационно-распорядительная документация

Название	Содержание
	Приложение 10 к Приказу. Инструкция по действию в случае компрометации ключевой информации.
Форма Акта внедрения средств защиты информации	Форма Акта соответствия
	Приложение 1. Настройки СЗИ
Приказ «О назначении комиссии по декларированию соответствия информационных систем персональных данных требованиям безопасности»	Определяет состав комиссии по проведению декларирования соответствия информационных систем персональных данных требованиям безопасности
	Приложение 1. Состав комиссии
	Приложение 2. Акт соответствия информационной системы персональных данных требованиям по безопасности

Техническое задание

Техническое задание на создание системы защиты персональных данных должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- класс ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;

Техническое задание

Техническое задание на создание системы защиты персональных данных должно содержать:

- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

ДиалОгНаука

Разработка организационно-распорядительной документации

Результаты этапа:

- Согласованный комплект организационно-распорядительных документов
- Техническое задание на создание системы защиты персональных данных компании

Длительность этапа: 1 месяц

ДиалОгНаука

Разработка организационно-распорядительной документации

Консультант:

- Разработка организационно-распорядительных документов
- Устранение замечаний и доработка документов в процессе их согласования с Заказчиком

Заказчик:

- Согласование организационно-распорядительных документов с соответствующими подразделениями компании

ДиалОгНаука

Проектирование системы защиты персональных данных

- Макетирование и стендовые испытания средств защиты информации

- Разработка технического проекта на создание системы защиты персональных данных, включая:
  - Пояснительную записку с описанием программно-технических решений по защите персональных данных
  - Ведомость покупных изделий

ДиалогНаука

Подсистемы защиты

- Требования к системам защиты для ИСПДн К2 и К3 **идентичны**
- Существенные дополнительные требования для ИСПДн **К1:**
  - Использование программного обеспечения СЗИ, соответствующего 4 уровню контроля отсутствия НДВ
  - Дополнительные требования по регистрации (выдачи на печать, доступа к защищаемым ресурсам и т.д.)
  - Очистка освобождаемых областей оперативной памяти и внешних накопителей
  - Дополнительные требования к межсетевому экранированию

ДиалОгНаука

Проектирование системы защиты персональных данных

Результаты этапа:

- Отчет по результатам проведенных стендовых испытаний средств защиты информации
- Технический проект на систему защиты персональных данных

Длительность этапа: 1 месяц

ДиалОгНаука

Проектирование системы защиты персональных данных

Консультант:

- Проведение макетирования и стендовых испытаний
- Разработка материалов технического проекта

Заказчик:

- Участие в подготовке стенда и проведении макетирования средств защиты информации
- Согласование материалов технического проекта на системы защиты персональных данных

ДиалОгНаука

Ввод в действие системы защиты персональных данных

- установка пакета прикладных программ в комплексе с программными средствами защиты информации;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации

ДиалОгНаука

Ввод в действие системы защиты персональных данных

Результаты этапа:

- Установленные и настроенные средства защиты информации
- Проведен инструктаж администраторов по эксплуатации средств защиты информации

Длительность этапа: Зависит от состава внедряемых средств защиты информации

ДиалОгНаука

Ввод в действие системы защиты персональных данных

Консультант:

- Установка и настройка средств защиты информации
- Проведение инструктажа администраторов Заказчика

Заказчик:

- Участие в процессе установки и настройки средств защиты информации
- Изучение особенностей эксплуатации средств защиты информации

Оценка соответствия ИСПДн

Возможные варианты оценки соответствия:

- Декларирование соответствия
- Аттестация информационной системы персональных данных

ДиалогНаука

Аттестация ИСПДн

- Для ИСПДн 1 и 2 классов – рекомендуется проведение аттестации по требованиям безопасности информации

Преимущества аттестации:

- Делегирование рисков несоответствия действующему законодательства органу по аттестации, выдавшему аттестат соответствия
- Упрощение процедуры проверки со стороны регуляторов

ДиалОгНаука

Оценка соответствия ИСПДн

Результаты этапа:

- Результаты оценки соответствия ИСПДн требованиям по безопасности информации

Длительность этапа: 2-4 недели (зависит от выбранной формы оценки соответствия)

ДиалОгНаука

Оценка соответствия ИСПДн

Консультант:

- Разработка документов, необходимых для проведения оценки соответствия
- Проведение оценки соответствия и оформление соответствующих результатов

Заказчик:

- Согласование результатов оценки соответствия

ПРИМЕРЫ ПРАКТИЧЕСКИХ РЕШЕНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ДиалогНаука

Защита персональных данных

- Антивирусная защита
- Криптографическая защита ПДн в процессе их хранения и передачи по сети
- Защита персональных данных от несанкционированного доступа
- Анализ защищённости ПДн
- Защита от информационных атак
- Мониторинг информационной безопасности

ДиалОгНаука

Состав предлагаемых средств защиты

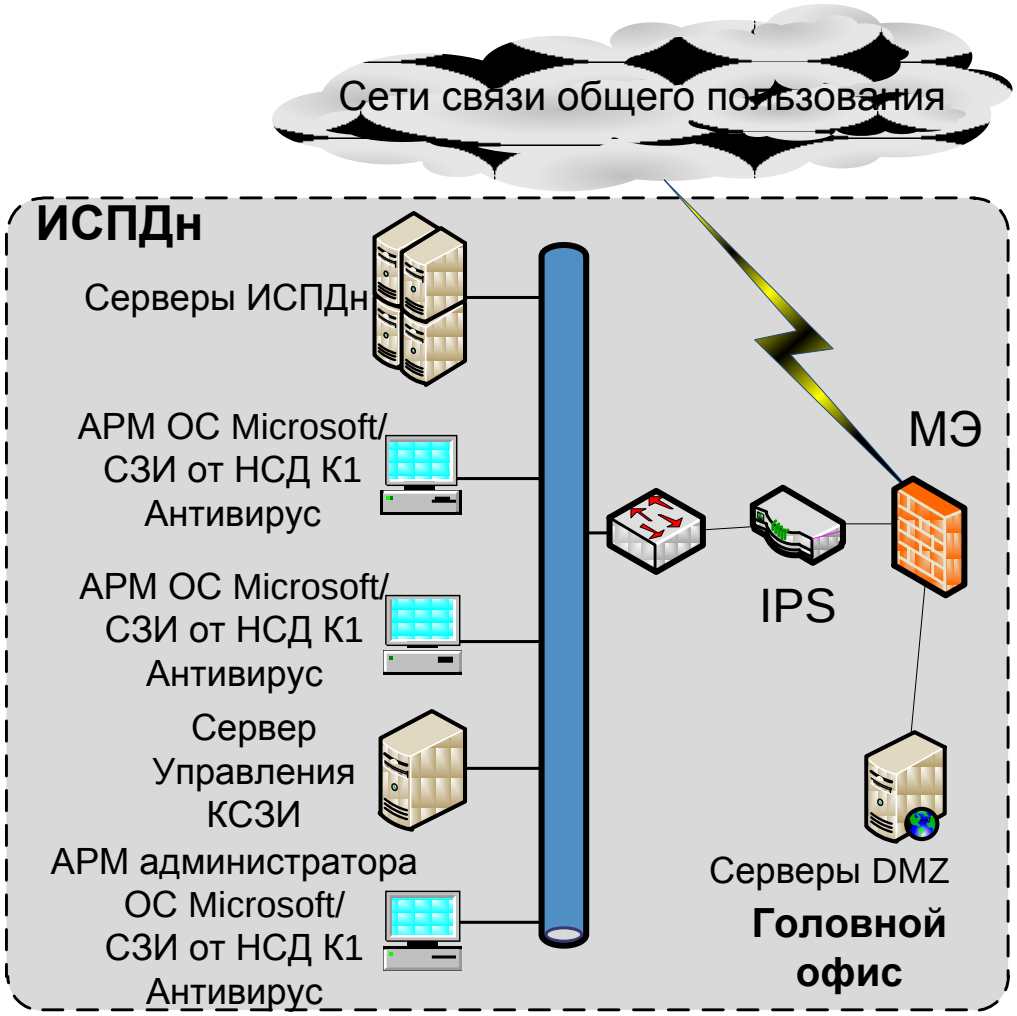
Подсистема	ИСПДн К1	ИСПДн К2 (К3)
Подсистема управления доступом	Панцирь-К, SecretNet	Пакет сертификации для ОС Microsoft, сертифицированные прикладные системы
Подсистема регистрации и учета	Панцирь-К, SecretNet	Пакет сертификации для ОС Microsoft, сертифицированные прикладные системы
Подсистема обеспечения целостности	Панцирь-К, SecretNet	Пакет сертификации для ОС Microsoft
Подсистема антивирусной защиты	Dr.Web, Антивирус Касперского, NOD 32, Symantec Endpoint Protection, TrendMicro	Dr.Web, Антивирус Касперского, NOD 32, Symantec Endpoint Protection, TrendMicro
Подсистема межсетевого экранирования	Континент, VipNet, С-Терра СиЭсПи, StoneGate	МЭ ISA, Check Point, Cisco

ДиалогНаука

Состав предлагаемых средств защиты

Подсистема	ИСПДн К1	ИСПДн К2 (К3)
Подсистема анализа защищенности	MaxPatrol, Xspider, Ревизор Сети	MaxPatrol, Xspider, Ревизор Сети
Подсистема обнаружения вторжений	Proventia Network IPS, StoneGate IPS	Proventia Network IPS, StoneGate IPS
Подсистема криптографической защиты информации	КриптоПро CSP (в составе С-Терра, StoneGate, Континент), ViPNet CSP	КриптоПро CSP (в составе С-Терра, StoneGate, Континент), ViPNet CSP

Локальная ИСПДн одного класса

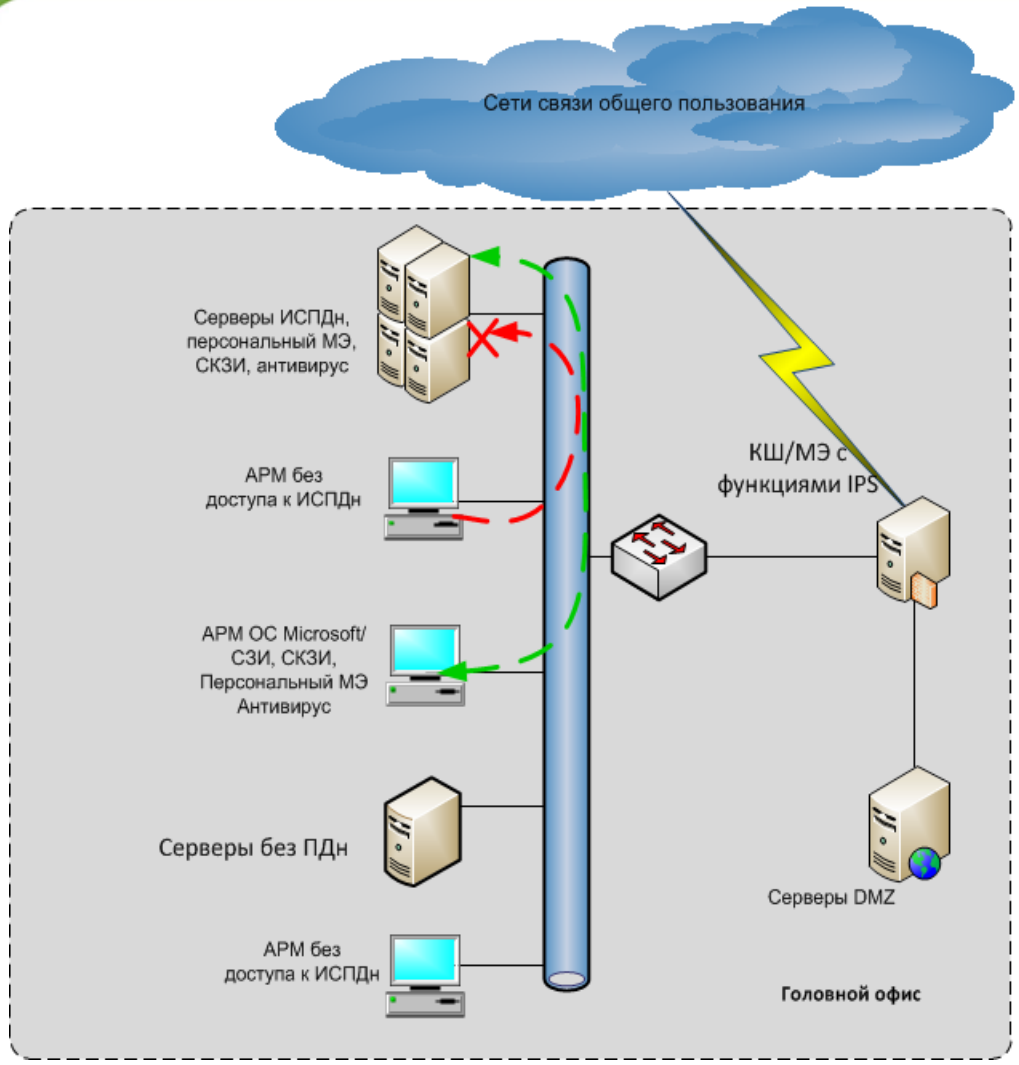


Оптимально в случаях:

- небольших компаний;
- все ИСПДн одного класса (К1 или К2(К3)), или когда большинство узлов относится к ИСПДн максимального класса
- когда стоимость разделения на сегменты больше стоимости защиты сети по максимальному классу

ДиалогНаука

«Наложенная» ИСПДн



Оптимально в случаях:

- Когда с ПДн работает небольшая часть сотрудников
- Невозможно внести изменения в структуру сети

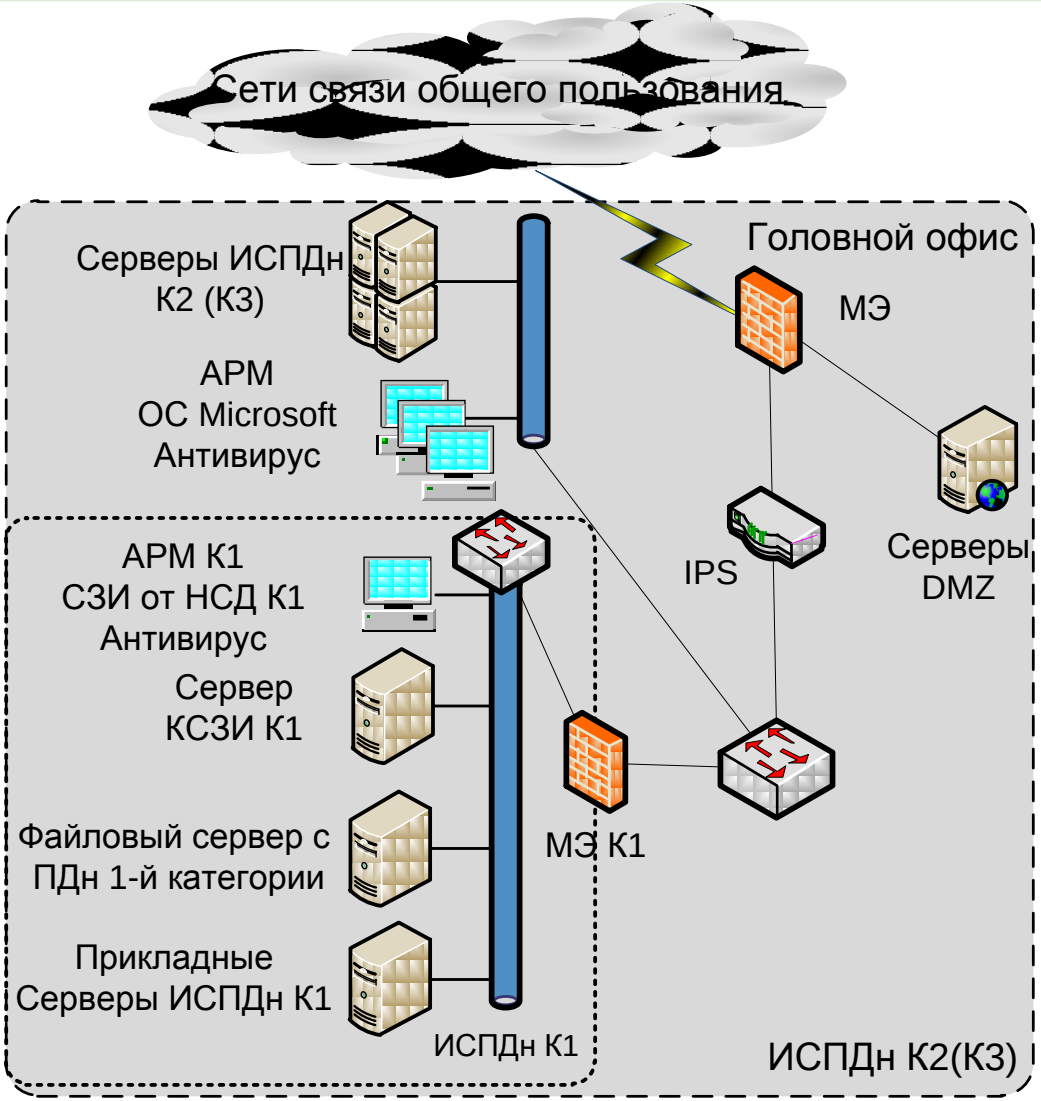
Существенные минусы:

- Очень ограниченный выбор решений, позволяющих осуществлять шифрованные соединения «клиент-клиент»

Примечание:

Возможна реализация схемы с выносом только серверов ИСПДн за КШ, в таком случае выбор решений многократно возрастает

Локальные ИСПДн разных классов



Оптимально в случаях:

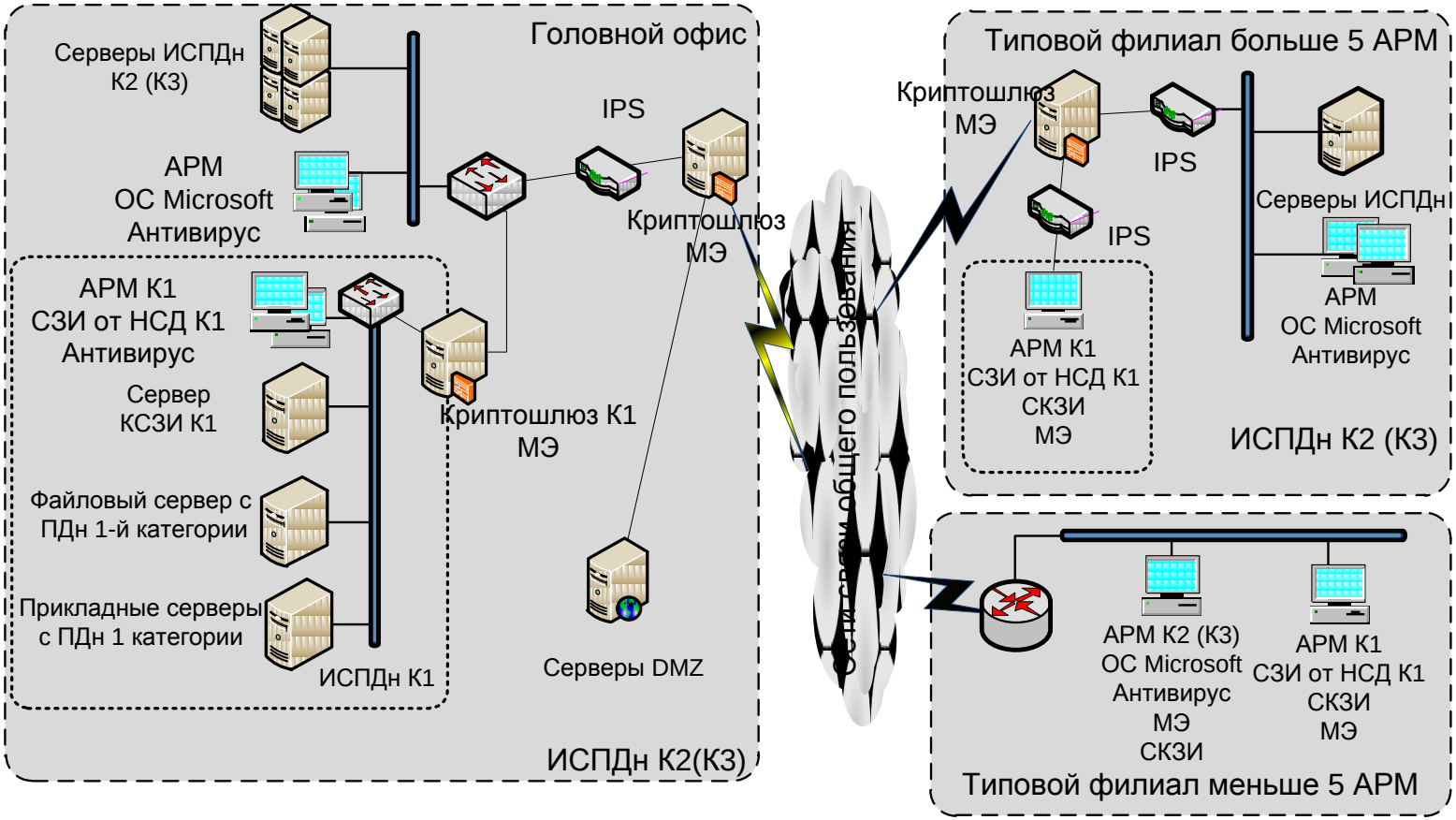
- Когда невозможно объединить ИСПДн разных классов;
- Количество рабочих станций К1 значительно меньше К2 (К3)

Существенные минусы:

- Необходимость физического разделения сегментов сети

ДиалОгНаука

Распределенная ИСПДн разных классов



ДиалОгНаука

Современные проблемы информационной безопасности

Большое количество разнородных устройств безопасности

- **90%** используют межсетевые экраны и антивирусы
- **40%** используют системы обнаружения вторжений (IDS)
- количество сетевых устройств растет
- больше оборудования означает большую сложность

Очень много событий по безопасности !

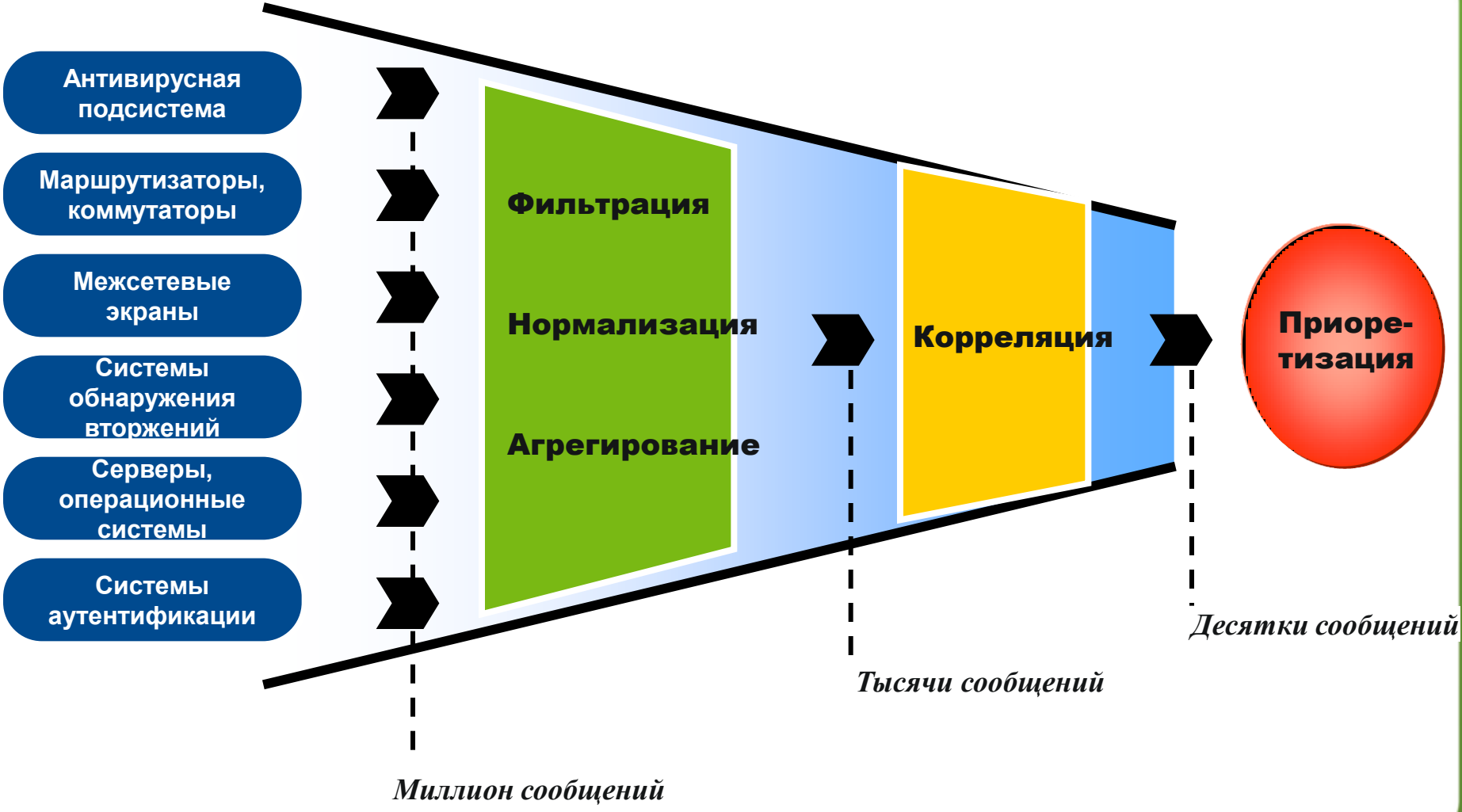
- один межсетевой экран может генерировать за день более 1 Гигабайта данных в Log-файле
- один сенсор IDS за день может выдавать до 50 тыс. сообщений, до 95% ложных тревог!
- сопоставить сигналы безопасности от разных систем безопасности практически невозможно

Слишком много устройств, слишком много данных…

Ответные действия на угрозы безопасности должны быть предприняты немедленно!

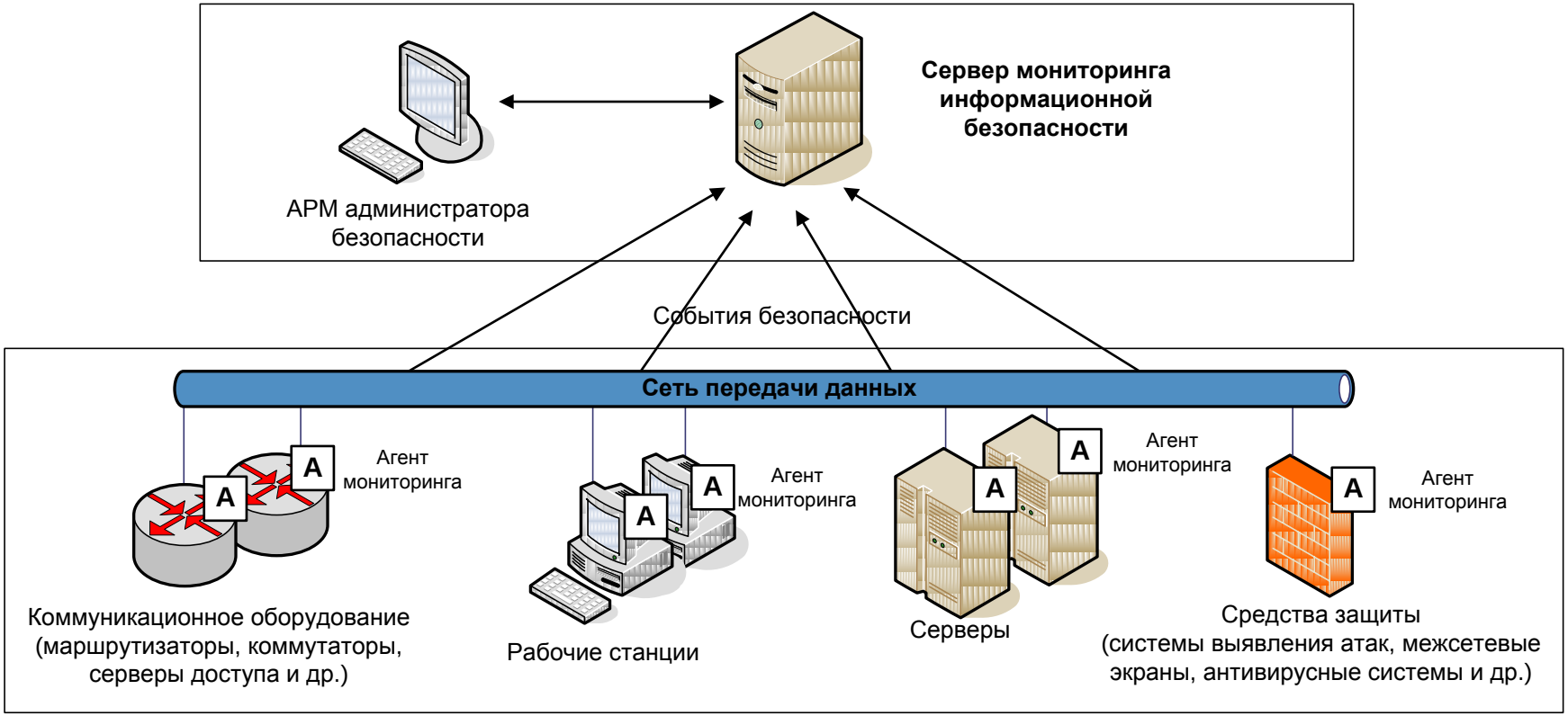
ДиалогНаука

Принцип работы SIEM



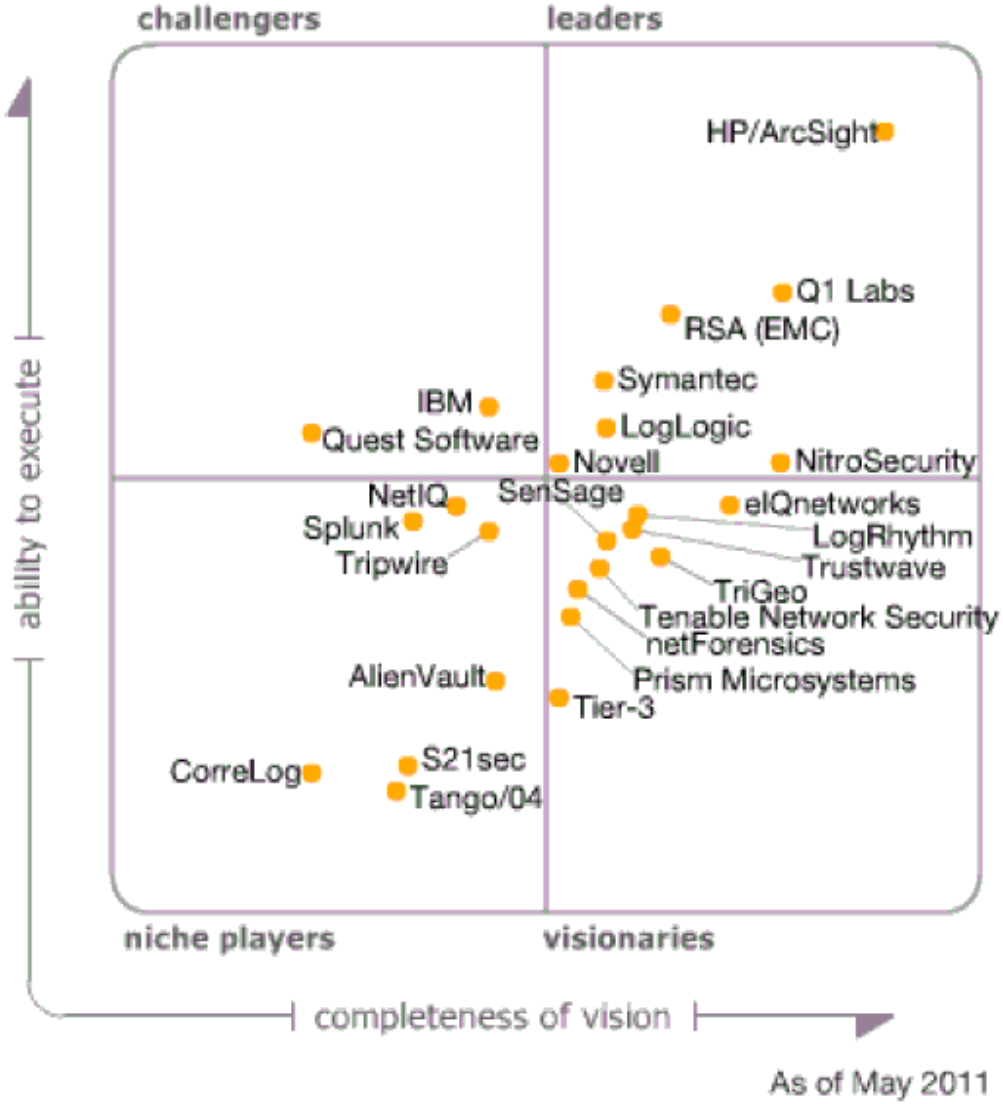
ДиалогНаука

Архитектура системы мониторинга



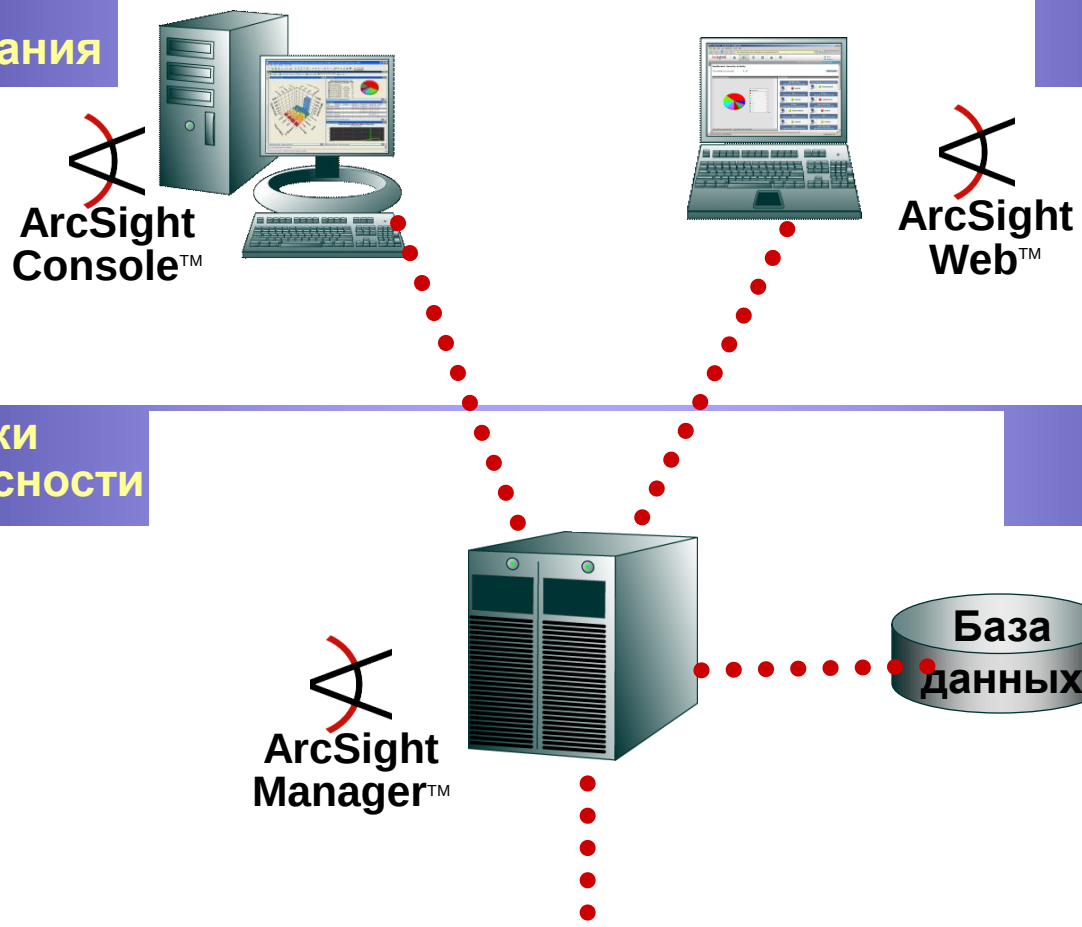
ДиалОгНаука

Отчет «Волшебные квадранты» по рынку SIEM, Gartner - 2011



ДиалОгНаука

ArcSight ESM Архитектура



ДиалогНаука

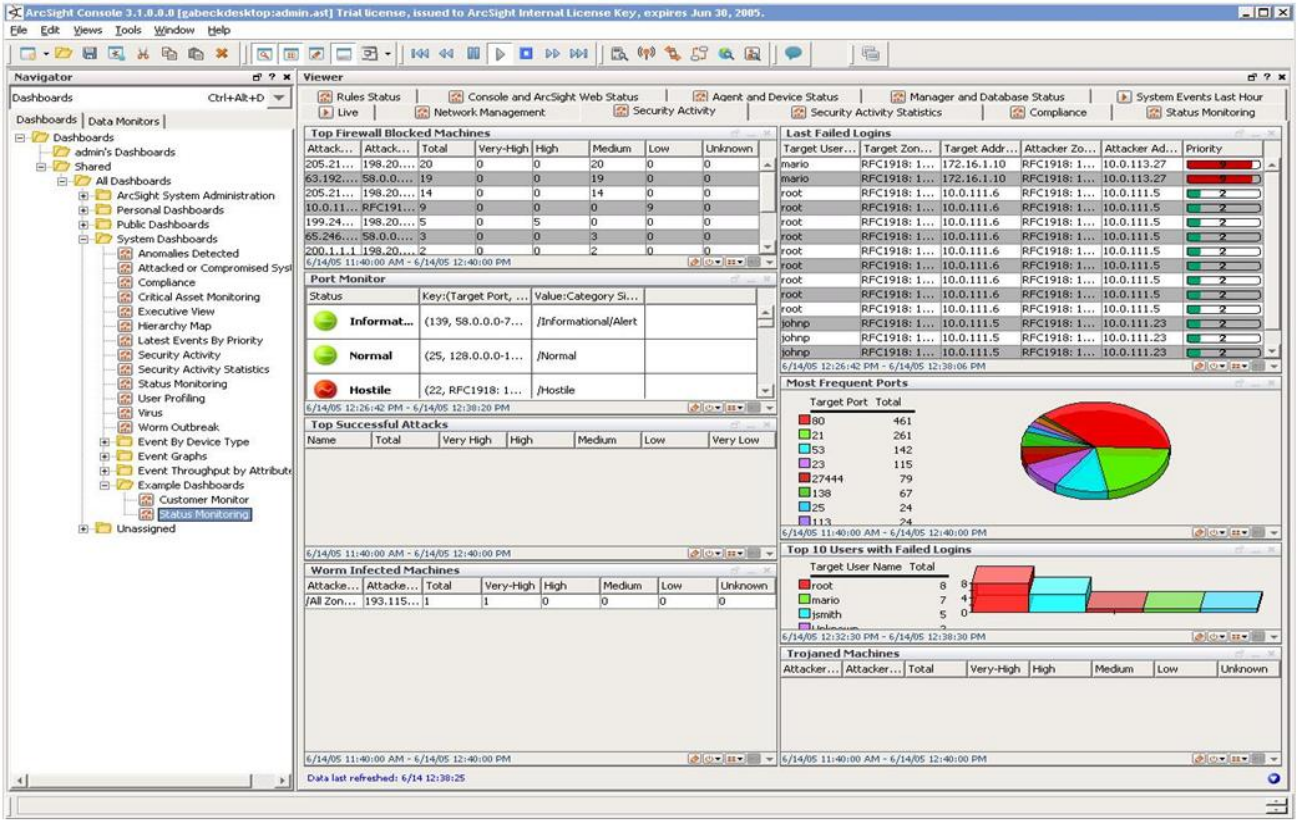
Поддерживаемые устройства

Access and Identity	Data Security	Integrated Security	Network Monitoring	Security Management	Web Cache
Anti-Virus	Firewalls	Log Consolidation	Operating Systems	Switch	Web Filtering
Applications	Honeypot	Mail Relay & Filtering	Payload Analysis	VPN	Web Server
Content Security	Host IDS/IPS	Mail Server	Policy Management	Vulnerability Mgmt	Wireless Security
Database	Network IDS/IPS	Mainframe	Router		

ДиалОгНаука

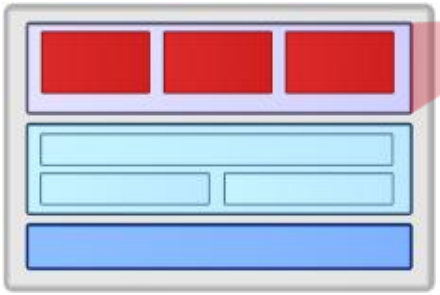
Визуализация
Консоль реального времени

- Разделение событий по категориям
- Возможность корреляции событий в реальном режиме времени, как по ресурсам, так и по злоумышленникам
- Возможности подробного анализа
- Возможность создания коррелированных отчетов



Категоризация событий обеспечивает мгновенную идентификацию атаки

Дополнительные пакеты ArcSight



Дополнительные пакеты ArcSight

- Набор правил, отчётов, графических панелей и коннекторов
- Стандарты: оценка соответствия стандартам и\или законодательству
- Бизнес: решение наиболее распространённых задач защиты информации

Доступны в виде:

Отдельного ПО

Стандарты:

SOX/JSOX IT Gov
PCI FISMA

Бизнес:

IdentityView
Fraud Detection
Sensitive Data Protection

Предустановленного устройства

ДиалогНаука

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: vas@DialogNauka.ru