

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КАТАЛОГ УСЛУГ
LETA IT-company



Настоящий документ был подготовлен LETA IT-company исключительно в информационных целях и содержит только краткие справочные данные о продуктах и услугах компании. Настоящий каталог не является офертой, публичной офертой, равно как и коммерческим предложением в какой-либо форме. Более подробную информацию о продуктах и услугах компании можно получить, обратившись к представителям LETA IT-company. Любое распространение всего документа или его части допускается лишь с письменного разрешения LETA IT-company. При цитировании документа ссылка на источник заимствования обязательна.

© LETA IT-company, 2010

Содержание

О LETA IT-company	04
Наш подход к обеспечению информационной безопасности	
Построение комплексной системы информационной безопасности	08
Методология выполнения проектов	10
Управление проектами	11
Контроль качества	12
Услуги и решения LETA IT-company в области управления ИБ	
Разработка стратегии информационной безопасности	14
Аудит ИБ	15
Построение Системы управления ИБ (СУИБ) в соответствии с ISO 27001	16
Построение системы инвентаризации и управления информационными активами	20
Построение системы управления уязвимостями	22
Построение системы сбора, корреляции событий и управления инцидентами ИБ	24
Построение системы внутреннего аудита и обеспечения соответствия требованиям	26
Построение системы управления информационными рисками	28
Построение системы обеспечения непрерывности бизнес-процессов	29
Услуги и решения LETA IT-company в области соответствия требованиям	
Обеспечение соответствия требованиям Федерального закона РФ № 152-ФЗ «О персональных данных»	32
Обеспечение соответствия требованиям PCI DSS	35
Обеспечение соответствия требованиям СТО БР ИББС	37
Услуги и решения LETA IT-company по обеспечению информационной безопасности	
Построение системы противодействия утечке конфиденциальной информации	40
Построение системы контроля устройств ввода-вывода информации	42
Построение корпоративной системы контроля входящего веб-трафика	44
Построение корпоративной системы шифрования данных	46
Построение корпоративной системы идентификации и аутентификации	48
Построение корпоративной инфраструктуры открытых ключей - PKI (Корпоративный Удостоверяющий центр - УЦ)	49
Построение системы антивирусной защиты серверов и рабочих станций	51
Построение корпоративной системы защиты каналов связи	53
Построение системы обнаружения и предотвращения вторжений	55
Построение корпоративной системы межсетевого экранирования	57
Построение системы удаленного защищенного доступа	59
Построение системы резервного копирования и восстановления данных	66
Построение системы архивирования корпоративной почты	63
Услуги по защите информационных ресурсов, собственником которых является государство (государственная тайна, конфиденциальная информация)	65
Стратегические партнеры LETA IT-company	67
О LETA Group	71

Информация о компании, компетенции

О LETA IT-company

LETA IT-company (www.leta.ru) – один из ведущих игроков рынка информационной безопасности в России. LETA оказывает заказчикам весь спектр услуг по информационной безопасности, начиная с разработки стратегии ИБ и заканчивая услугами по внедрению и сопровождению технических средств защиты информации. Портфель услуг LETA IT-company включает защиту персональных данных, защиту от утечек информации, обеспечение безопасности при работе в сети Интернет, аудит ИБ и построение систем управления ИБ в соответствии с требованиями российских и международных стандартов, защиту от вирусов, спама, атак и вторжений, контроль уязвимостей. LETA IT-company входит в состав LETA Group – компании №1 по объему продаж на российском рынке продуктов и услуг в сфере информационной безопасности по данным рейтинга «CNews Security 2009: Крупнейшие ИТ-компании России в сфере защиты информации».

LETA IT-company занимает 3-е место среди крупнейших ИТ-компаний России в сфере защиты информации и является лидером российского рынка защиты от утечек данных и борьбы с инсайдерами (Data Loss/Leak(age) Prevention – DLP).

LETA IT-company применяет в работе комплекс инновационных подходов, обеспечивающих заказчикам дополнительные выгоды и преимущества сотрудничества, среди которых:

- модель типизированных услуг;
- система управления проектами;
- система управления качеством;
- комплексная система обучения;
- система управления по целям.

LETA IT-company является партнером ведущих зарубежных и российских вендоров в сфере информационной безопасности и информационных технологий. В рамках многолетнего сотрудничества с ключевыми производителями LETA обладает высокими партнерскими статусами различного уровня, в частности:

- Platinum Partner от Symantec;
- Gold ChannelConnect Partner от Websense;
- Security Alliance Elite Partner от McAfee;
- AffinityPlus Partner от Trend Micro;
- Bronze Partner от Check Point;
- Gold Certified Partner от Microsoft (с компетенцией *Security Solutions* в числе других).

Компетенция LETA IT-company

Лицензии ФСБ России:



- Лицензия ФСБ России на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с применением шифровальных (криптографических) средств информационных и телекоммуникационных систем. Рег. № 8037 П от 01 декабря 2009 г.
- Лицензия ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств. Рег. № 8038 Х от 01 декабря 2009 г.
- Лицензия ФСБ России на осуществление распространения шифровальных (криптографических) средств. Рег. № 8039 Р от 01 декабря 2009 г.
- Лицензия ФСБ России на осуществление предоставления услуг в области шифрования информации. Рег. № 8040 У от 01 декабря 2009 г.

Лицензии ФСТЭК России:



- Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации. Регистрационный № 0943 от 30 ноября 2009 г.
- Лицензия ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации. Регистрационный № 0571 от 30 ноября 2009 г.



LETA входит в сообщество ABISS, объединяющее пользователей стандартов Центрального Банка Российской Федерации по обеспечению информационной безопасности организаций банковской системы РФ.



Является авторизованным партнером BSI (British Standards Institution) со статусом BSI Certified Partner.



LETA IT-company входит в консорциум с компанией Digital Security, обладающей статусом QSA (Qualified Security Assessor), что позволяет LETA оказывать услуги по выполнению требований PCI DSS.

Наш подход к
обеспечению
информационной
безопасности

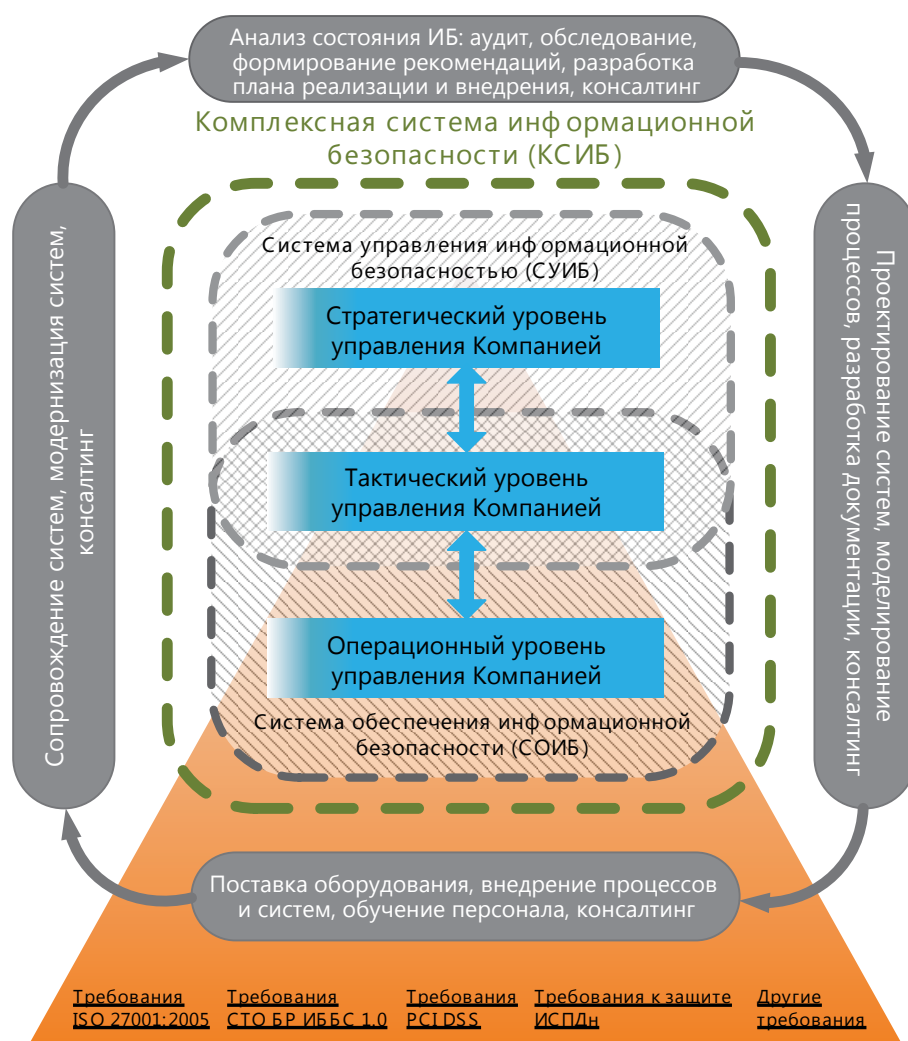
Построение комплексной системы информационной безопасности

Современные организации обладают, как правило, сложной, территориально распределенной корпоративной информационной системой и большим количеством критичных информационных ресурсов и работают в условиях растущих репутационных рисков и непрерывно меняющихся внешних требований.

В такой ситуации обеспечить безопасность информации при адекватных расходах возможно лишь при использовании системного подхода, который подразумевает последовательное внедрение в компании комплексной системы информационной безопасности (КСИБ).

Наличие КСИБ позволяет снизить правовые, финансовые, репутационные и операционные риски, связанные с безопасностью информации, обеспечить соответствие всем актуальным для организации требованиям, оптимизировать организационную структуру и финансовые расходы на обеспечение информационной безопасности.

КСИБ включает в себя набор взаимосвязанных организационных мер, программно-технических средств и процессов управления на всех уровнях деятельности организации: стратегическом, тактическом и операционном.



LETA IT-company предлагает полный спектр услуг и решений, необходимых для построения КСИБ. Среди них можно выделить три основных направления:

- услуги и решения по управлению ИБ;
- услуги по обеспечению ИБ;
- услуги по обеспечению соответствия требованиям.

Услуги и решения по управлению ИБ направлены на построение в организации эффективных процессов управления, которые обеспечивают:

- предоставление максимально полной и достоверной информации о состоянии информационной безопасности на всех уровнях управления организацией;
- эффективный обмен информацией между всеми заинтересованными сторонами: руководством организации, акционерами, клиентами и партнерами, регулирующими органами и органами по сертификации;
- принятие правильных и своевременных решений на всех уровнях управления организацией в условиях внешних и внутренних изменений;
- оптимизацию финансовых расходов на информационную безопасность.

Услуги и решения по обеспечению ИБ направлены на защиту информационной системы организации от внешних и внутренних угроз информационной безопасности, в том числе:

- угроз несанкционированного доступа и несанкционированного использования информационных ресурсов;
- угроз утечки и разглашения конфиденциальной информации;
- угроз, возникающих при взаимодействии с сетью Интернет и другими внешними сетями;
- угроз нарушения целостности или доступности информационных ресурсов;
- других угроз информационной безопасности.

Услуги и решения по обеспечению соответствия требованиям направлены на защиту информации в соответствии с актуальными требованиями законодательства РФ, контролирующих, регулирующих и сертификационных органов, в том числе:

- с Законом № 152-ФЗ «О персональных данных»;
- стандартом международных платежных систем PCI DSS;
- стандартом Банка России СТО БР ИББС;
- международным стандартом ISO IEC 27001:2005;
- другими требованиями в области информационной безопасности.

Комплексный проект по обеспечению ИБ может включать нескольких связанных друг с другом решений из разных направлений.

Методология выполнения проектов

В рамках реализуемых проектов LETA IT-company проводит полный цикл работ по построению систем информационной безопасности:

- обследование и анализ состояния информационной безопасности организации;
- проектирование систем, моделирование процессов, разработка документации;
- поставка оборудования, внедрение процессов и систем, обучение персонала;
- сопровождение систем и процессов ИБ.

При выполнении проектов особое внимание мы уделяем взаимодействию и обучению специалистов Заказчика, т.к. наличие квалифицированных специалистов является ключевым фактором для успешного внедрения и последующего эффективного функционирования внедряемых процессов и систем.

При внедрении программно-технических решений мы широко используем технологии виртуализации, что позволяет сократить количество физических серверов, требуемых для установки ПО, и существенно повысить масштабируемость, безопасность и отказоустойчивость решения.

Предпроектное обследование и анализ состояния информационной безопасности организации

Обследование проводится с целью анализа состояния информационной безопасности организации и уточнения требований к внедряемому решению. Оно включает в себя сбор и обработку информации об организационной структуре, процессах и процедурах, программно-технических решениях, имеющихся у Заказчика, а также об актуальных для него внешних и внутренних требованиях. По результатам этапа обследования разрабатывается проектное (техническое) задание на внедрение требуемых организационных мер, программно-технических средств и процессов управления.

Также, в случае необходимости, на этом этапе могут быть разработаны политики информационной безопасности, определяющие основные требования к обеспечению ИБ в организации.

Проектирование систем и моделирование процессов

На этапе проектирования разрабатывается технический проект внедряемого решения. Проектирование выполняется в соответствии с требованиями ГОСТ 32.

Также, в случае необходимости, на этом этапе проводится проектирование (моделирование) процессов и процедур и их тестирование, что позволяет обнаружить и устранить возможные проблемы и узкие места на раннем этапе, избежать ошибок и значительных изменений на этапе внедрения и, таким образом, снизить риски проекта.

При проектировании систем, входящих в состав интеграционного решения, проводится пилотное тестирование на площадке Исполнителя с целью проверки совместимости входящих в него технических решений, а также, в случае необходимости, разработки и тестирования входящих в него дополнительных программных компонентов (коннекторов, скриптов и т.п.).

Поставка оборудования, внедрение процессов и систем, обучение персонала

На этапе внедрения осуществляется поставка и развертывание программно-технических средств на площадках Заказчика в соответствии с разработанным техническим проектом, а также, в соответствии с разработанными моделями процессов и процедур, проводится обучение персонала Заказчика и формируется необходимая рабочая документация (регламенты, инструкции, перечни, схемы и т.п.).

В случае, если техническое решение затрагивает бизнес-процессы организации в значительной степени, внедрение проводится постепенно с выделением пилотной зоны на площадке Заказчика и последующим поэтапным распространением решения на всю область деятельности, охватываемую проектом.

По завершении этапа внедрения проводятся тестовые испытания внедренного решения в соответствии с разработанными на этапе проектирования программой и методикой испытаний и приемка систем в промышленную эксплуатацию.

Сопровождение систем и процессов ИБ

Для обеспечения максимальной надежности и доступности внедренного решения LETA IT-company предлагает услугу по расширенной технической поддержке, которая включает в себя поддержку по телефону, а также возможные выезды к Заказчику.

Услуга по сопровождению внедренного решения может также включать в себя консультационную поддержку и инспекционные визиты для оценки эффективности функционирования внедренных процедур и программно-технических средств и устранения выявленных проблем.

Управление проектами

Проектная деятельность Исполнителя основана на лучших мировых практиках (PMI PMBOK), а также на собственном опыте реализации проектов. Все проекты Исполнителя реализуются в соответствии с Корпоративной системой управления проектами (далее — КСУП). При реализации проекта Руководитель проекта и все участники проектной команды должны четко следовать регламентированным в КСУП требованиям. Профессионализм участников проектных команд и строгое соблюдение формализованных требований позволяет обеспечить высокое качество оказываемых консалтинговых услуг и услуг по внедрению технических средств.

Главными критериями успешного выполнения проектов служат уровень удовлетворённости Заказчика качеством оказываемых услуг и сбалансированность ключевых показателей по сроку, бюджету и содержанию проекта.

В рамках коммуникаций при реализации проекта Руководители проектов со стороны Исполнителя и Заказчика являются ключевым звеном.

Схема коммуникаций приведена ниже.



Контроль качества

Контроль качества проектов Исполнитель реализовывает четырьмя независимыми контурами:

- **двухступенчатый внутренний контроль качества проекта осуществляется:**
 - руководителем проекта;
 - руководством Департамента внедрения и консалтинга;
- **двухступенчатый внешний контроль качества проекта включает:**
 - внешний контроль качества отделом качества;
 - измерение восприятия Заказчиком достигнутого в проекте качества.

Первые два контрольных контура, которые курируют руководители, ответственные за выполнение проекта, решают задачу максимально быстрого обнаружения возможных отклонений от запланированных показателей проекта, а также позволяют оперативно разрешать возникающие при выполнении проекта нестандартные ситуации и принимать предупреждающие и корректирующие меры.

Для получения максимально объективной информации по проекту, независимой от исполнителей работ, проводится независимый контроль качества сотрудниками отдела качества, подчиненными непосредственно Руководству Исполнителя. Такие аудиты качества проводятся в ходе проекта с момента его инициации и вплоть до закрытия для проверки исполнения требований, установленных:

- в нормативных документах по управлению проектами;
- в договорной документации;
- в иных документах, которые могут содержать требования, в том числе порождаемых в ходе проекта.

Кроме контроля исполнения установленных требований выполняется измерение восприятия клиентом достигнутого качества результатов проекта. Такие проверки выполняются сотрудниками отдела качества методом интервьюирования представителей Заказчика, курирующих проект (при личной встрече либо в ходе телефонного разговора). Проверки могут проводиться по результатам этапов проекта и обязательно после завершения проекта, после подписания последнего акта выполненных работ. В случае возникновения непредвиденных ситуаций, которые не удается разрешить силами проектной команды, Руководство Исполнителя может принять решение о независимом измерении восприятия Заказчиком сложившейся ситуации.

Результаты независимых аудитов качества и измерений восприятия Заказчика по достигнутому качеству выносятся на рассмотрение комитета по качеству под председательством Генерального директора Исполнителя. Помимо принятия оперативных мер реагирования, информация проверок используется Руководством Исполнителя для принятия решений по совершенствованию деятельности и улучшению качества услуг.

Также сотрудники Заказчика, курирующие проект, могут высказать свою претензию по телефону или, оформив ее в письменном виде, отправить по электронной почте непосредственно в отдел качества Исполнителя, который обязан незамедлительно организовать ее рассмотрение и не позднее 10 дней дать официальный ответ на поданную претензию.

Услуги и решения LETA в области управления ИБ

Разработка стратегии информационной безопасности

Формирование общей стратегии компании подразумевает определение частных стратегических целей для всех областей деятельности, в том числе для процесса обеспечения информационной безопасности.

Правильно разработанная стратегия информационной безопасности позволяет ответить на важные вопросы:

- В каком состоянии находится информационная безопасность сейчас, и в каком направлении необходимо двигаться дальше?
- Какие из задач информационной безопасности наиболее приоритетны?
- Как распределять инвестиции?
- Что именно нужно сделать для решения поставленных задач?
- Как именно должна работать служба информационной безопасности, чтобы достичь поставленных целей?
- Как оценивать эффективность выполнения задач стратегии?
- Как избежать конфликтов между долгосрочными и краткосрочными целями?
- Что нужно сделать, чтобы стратегия реализовывалась, а не была всего лишь еще одним неработающим документом?

Эти вопросы становятся особенно актуальными в период, когда в компании происходят значительные изменения. Пересмотр стратегии информационной безопасности необходим в случае смены стратегического курса компании, при слиянии или поглощении, в случае смены владельцев или высшего руководства.

Разработка стратегии информационной безопасности одновременно со стратегией ИТ позволяет избежать впоследствии значительных затрат на изменение уже построенной ИТ-инфраструктуры в угоду требованиям по информационной безопасности.

Услуга по разработке стратегии информационной безопасности включает следующие работы:

- анализ стратегии бизнеса, кадровой стратегии и стратегии ИТ;
- анализ законодательных требований и требований регулирующих органов, действующих в отношении компании, в области информационной безопасности;
- разработка, оценка и выбор стратегических альтернатив;
- определение основных стратегических целей ИБ;
- определение задач, решение которых необходимо для реализации поставленных целей;
- формирование плана реализации стратегических задач и бюджетная оценка стоимости их выполнения.

Также в рамках проекта по разработке стратегии ИБ может быть создана система сбалансированных показателей (ССП) информационной безопасности, интегрированная в общую ССП компании и позволяющая контролировать выполнение стратегии ИБ в рамках единого процесса стратегического управления.

Работы по созданию стратегии ИБ проводятся экспертами по информационной безопасности с привлечением консультантов в областях стратегического планирования, управления бизнес-процессами, риск-менеджмента и внутреннего контроля.

При выполнении проекта используются современные методики, а также, если требуется, специализированные программные средства, позволяющие автоматизировать этап разработки стратегии, поддержание ее в актуальном состоянии и контроль ее выполнения.

Аудит ИБ

Аудит информационной безопасности представляет собой всестороннее обследование, позволяющее оценить текущее состояние информационной безопасности организации и спланировать дальнейшие шаги по повышению уровня защищенности.

Аудит информационной безопасности целесообразно проводить в случаях, когда нужна актуальная информация и независимая оценка состояния информационной безопасности.

Необходимость в этом может возникнуть в разных ситуациях:

- если меняется стратегия компании;
- при слиянии или поглощении;
- когда происходят значительные изменения в организационной структуре или смена руководства;
- при появлении новых внутренних или внешних требований в области информационной безопасности;
- в случае значительных изменений бизнес-процессов или ИТ-инфраструктуры.

Аудит может проводиться как для компании в целом, так и для отдельных критичных областей, бизнес-процессов или информационных систем.

Работа проводится экспертами, обладающими квалификацией, подтвержденной международными сертификатами, и обладающими богатым опытом проведения аудитов в различных отраслях экономики.

Методика выполнения работ предполагает гибкость и индивидуальный подход, позволяет учесть специфичные требования и особенности бизнеса каждой конкретной организации.

В процессе аудита обычно проводятся:

- анализ организационно-распорядительных документов организации;
- интервью с сотрудниками организации: представителями бизнес-подразделений, администраторами и разработчиками информационных систем, специалистами по информационной безопасности;
- осмотр технологических и офисных помещений с точки зрения обеспечения физической безопасности ИТ-инфраструктуры;
- анализ конфигурационных настроек оборудования и ПО;
- аудит с использованием специальных технических средств (сканеров анализа защищенности, средств контроля утечек информации и т.п.);
- тестирование на проникновение;
- оценка знаний сотрудников организации в области информационной безопасности.

Также могут быть выполнены дополнительные специальные проверки, позволяющие учесть особенности организации, в которой проводится аудит.

Результатом аудита могут являться:

- анализ угроз, которые могут быть реализованы, через обнаруженные уязвимости;
- качественная или количественная оценка рисков ИБ;
- оценка соответствия актуальным требованиям;
- оценка соответствия лучшим практикам и стандартам в области ИБ;
- стратегия обеспечения ИБ;
- рекомендации, которые должны быть выполнены для повышения уровня защищенности организации;
- план реализации разработанных рекомендаций с бюджетной оценкой;
- техническое задание на внедрение рекомендуемых мер по обеспечению информационной безопасности.

В случае необходимости на этапе обследования может быть собрана дополнительная информация, необходимая для выполнения других проектов, что позволит в дальнейшем сэкономить ресурсы организации и равномерно распределить расходы бюджета.

Построение Системы управления ИБ (СУИБ) в соответствии с ISO 27001

Система управления информационной безопасностью (СУИБ) обеспечивает объединение всех применяемых на предприятии защитных и организационных мер в единый адекватный реальным угрозам и управляемый комплекс, позволяющий достигать корпоративных целей информационной безопасности на уровне всего предприятия.

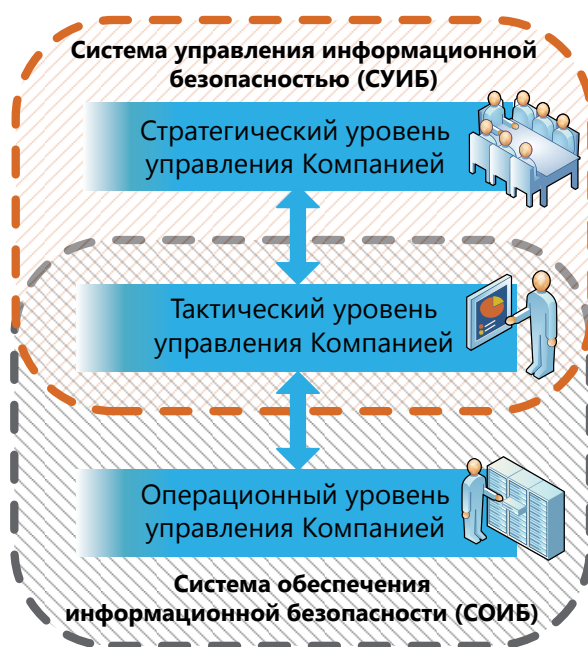


Рисунок. Место СУИБ в организации

Построение СУИБ позволяет четко определить, как взаимосвязаны процессы и подсистемы ИБ, кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования, и т.д.

Система управления информационной безопасностью выстраивается в соответствии с международным стандартом BS ISO/IEC 27001 и обеспечивает Заказчику ряд выгод от внедрения СУИБ и прохождения сертификационного аудита.

Выгоды Заказчика от внедрения СУИБ:

- выявление угроз безопасности для бизнес-процессов;
- снижение финансовых рисков и рисков прямых потерь Компании, повышение текущего уровня защищенности;
- управляемая и контролируемая система менеджмента ИБ;
- систематизация процессов обеспечения ИБ;
- достижение адекватности системы ИБ существующим рискам;
- расстановка приоритетов Компании в области ИБ;
- оптимизация и обоснование расходов на информационную безопасность;
- снижение операционных затрат за счет формализации процессов ИБ;
- достижение «прозрачности» в обеспечении ИБ и управлении информационными системами Компании;
- обеспечение соответствия уровня ИБ законодательным, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса;

- повышение доверия партнеров и клиентов Компании за счет демонстрации высокого уровня зрелости обеспечения ИБ всем заинтересованным сторонам;
- снижение операционных рисков (повышение экономической эффективности);
- снижение рисков для инвесторов (повышение прозрачности процессов внутри Компании);
- СУИБ – поставщик информации для всех заинтересованных сторон;
- повышение стоимости акций при выходе на IPO;
- повышение доверия клиентов, партнеров и заказчиков за счет демонстрации сертификата;
- меньше ресурсов и вложений в ИБ при слиянии компаний;
- проще пройти финансовый аудит (ИТ-аудит сопровождения);
- экономия времени, ресурсов и затрат на начальной стадии сбора информации при проведении любых внешних аудитов (в т.ч. аудитов Центробанка и финансовых аудитов).

Выгоды от сертификации СУИБ на соответствие требованиям ISO 27001:2005

- сертификация демонстрирует:
 - о акционерам и собственникам: что организация способна продолжать вне зависимости от обстоятельств оказание ключевых сервисов и выпуск основной продукции;
 - о организация соответствует требованиям действующего законодательства, регулирующих положений и контрактных условий;
- сертификация глобально подтверждает последовательность и устойчивость внедренных практик менеджмента;
- защищает интересы акционеров и собственников;
- повышает репутацию бренда;
- позволяет снизить расходы по оценке надежности поставщиков;
- помогает разработать, внедрить, обслуживать и совершенствовать систему менеджмента — испытанный подход предупреждающего характера к снижению рисков;
- постоянное совершенствование достигается благодаря регулярной экспертной оценке системы менеджмента;
- демонстрирует, что организация совершенствует и оттачивает действия персонала в случае возникновения чрезвычайной ситуации;
- ставит цели, к которым можно и необходимо стремиться;
- упрощает процесс внутренних и внешних аудитов;
- добавляет ценность бизнесу, помогая идентифицировать области и возможности для улучшения;
- помогает снижать расход благодаря меньшему количеству аудитов и проверок;
- снижает размер страховой премии по страхованию операционных рисков;
- сертификация демонстрирует приверженность организации принципам непрерывности бизнеса (защиты информации) и является инвестицией в выживание организации и повышение ее конкурентоспособности.

В рамках построения системы управления информационной безопасностью мы оказываем следующие услуги:

- обследование на соответствие требованиям ISO 27001:2005;
- построение систем управления информационной безопасностью (СУИБ) в соответствии с ISO 27001:2005;
- построение процессов управления ИБ:
 - о система управления рисками ИБ;
 - о система управления инцидентами ИБ;
 - о система внутреннего аудита и контроля соответствия;
 - о система управления уязвимостями;
 - о система управления активами и т.д.;
- подготовка СУИБ к сертификации на соответствие требованиям ISO 27001:2005;
- пакет поддержки СУИБ.



Обследование на соответствие требованиям ISO 27001:2005 позволяет определить, насколько текущая система управления организации соответствует требованиям ISO 27001:2005, при этом для каждого процесса обеспечения или управления ИБ определяется степень зрелости, а также разрабатываются рекомендации для соответствия требованиям ISO 27001:2005. На основании полученных результатов формируется план-график разработки и внедрения СУИБ.

Построение системы управления информационной безопасностью (СУИБ) в соответствии с ISO 27001:2005 предполагает проведение полного комплекса работ от планирования СУИБ до сертификационного аудита, а именно:

- разработку и внедрение процессов управления ИБ и, при необходимости, процессов обеспечения ИБ;
- разграничение ответственности между подразделениями ИТ и ИБ в рамках выполнения процессов СУИБ;
- разработку полного комплекта документации по ИБ в соответствии с требованиями стандарта;
- проведение анализа рисков ИБ и разработку плана-графика снижения рисков ИБ до приемлемого уровня;
- обучение персонала процессам и документации ИБ;
- подготовку системы к прохождению сертификационного аудита, включая взаимодействие с сертификационным органом, оказание консалтинговых услуг при устранении несоответствий, выявленных в ходе аудита.

В ходе проектирования СУИБ – этапа с основным объемом работ – определяется матрица видов и форматов информации и применяемых к ним защитных мер. Результаты этапа (положения о применимости контролей, план обработки рисков) позволяют перейти к завершающей стадии проекта построения СУИБ – внедрению.

Результатом проекта для Заказчика является СУИБ, готовая к сертификации на соответствие требованиям стандарта BS ISO/IEC 27001.

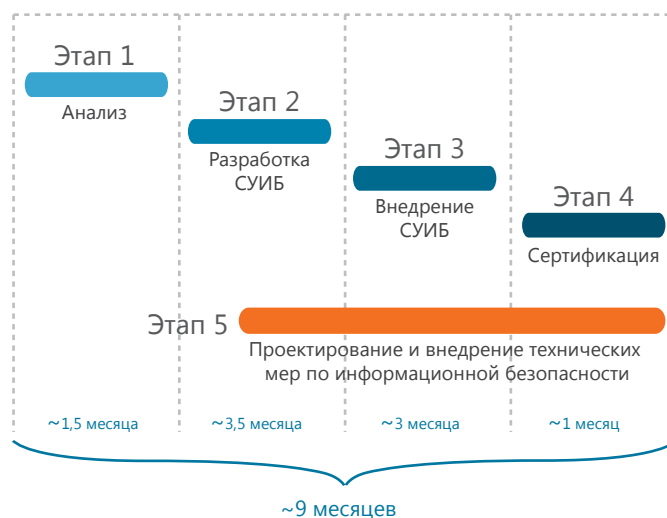


Рисунок. Этапы построения системы управления информационной безопасностью

Построение процессов управления ИБ производится в случае необходимости выстроить внутри компании отдельные элементы СУИБ. Каждый процесс повторяет по своей организации саму систему управления и включает в себя контрольные механизмы, распределение ответственности в рамках процесса, документирование с различной степенью детализации в зависимости от потребности Заказчика, обучение персонала, поставку и внедрение технических средств.

Подготовка СУИБ к сертификации на соответствие требованиям ISO 27001:2005 особенно актуальна, если Заказчик уже начинал своими силами строить систему, но по различным причинам в процессе выполнения проекта принял решение пригласить внешних консультантов. При этом нашими специалистами проводится анализ текущей ситуации и определяется степень необходимых доработок. В зависимости от глубины и детальности доработок формируется план-график подготовки СУИБ к сертификации на соответствие требованиям ISO 27001:2005.

Пакет поддержки СУИБ включает в себя работы, индивидуально подобранные для каждого Заказчика, которые позволяют обеспечить работоспособность процессов СУИБ на заданном уровне или повысить уровень зрелости отдельных процессов ИБ. В пакет поддержки могут быть включены работы по ежегодному проведению анализа рисков, оказание консалтинговой поддержки при проведении внутренних аудитов, разработка показателей эффективности для внедренных процессов, документирование отдельных элементов системы, организация курсов по информационной безопасности для сотрудников по области деятельности и т.д. Фактически любой процесс СУИБ может быть передан нашим специалистам на аутсорсинг, при этом в индивидуальном порядке определяется удобная для Заказчика форма взаимодействия: может быть организован центр компетенции, удаленное консультирование, проведение работ на площадке Заказчика и т.д.

Мы оказываем наши услуги по двум схемам выполнения работ:

Консалтинг по схеме «Под ключ». В соответствии с данной схемой работ наши специалисты проводят все работы на проекте самостоятельно, привлекая сотрудников Заказчика только для согласования результатов и обучения. Данная схема работ обеспечивает максимально качественное и своевременное выполнение проекта.

Консалтинг с разделением функций. Данная схема работ позволяет разделить работы проекта между ответственными исполнителями со стороны Заказчика и консультантами LETA IT-company. Разделение может быть проведено как вертикальное, так и горизонтальное. Вертикальное разделение позволяет ограничить область проведения проекта, горизонтальное разделение позволяет ограничить набор работ, которые будут выполнять на проекте специалисты Заказчика. При этом консультанты LETA IT-company проводят обучение специалистов Заказчика принципам выполнения работ. Данная схема работ позволяет уменьшить стоимость проекта и получить внутри компании обученных компетентных специалистов.

Построение системы инвентаризации и управления информационными активами

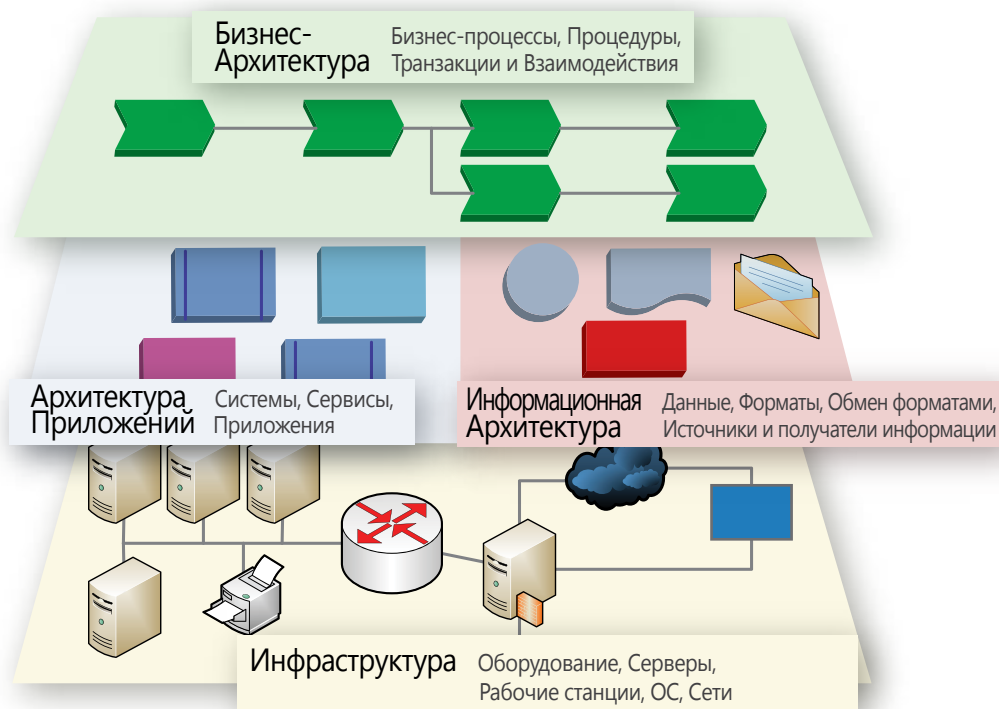
Используемые технические решения:

- Altiris Asset Management Suite/Inventory Solution
- ARIS IT Architect/Inventory
- MaxPatrol

Важнейшим фактором для успешного обеспечения информационной безопасности является наличие максимально полной, актуальной, достоверной и непротиворечивой информации о процессах обработки информации и поддерживающей их ИТ-инфраструктуре.

В условиях сложной распределенной ИТ-инфраструктуры поддержание актуальности информации об имеющихся информационных активах и управление изменениями является отдельной сложной задачей, для решения которой LETA IT-company предлагает внедрение специальных программных средств.

Использование специальных инструментов позволяет для бизнес-процессов, сервисов, информационных потоков, поддерживающей их ИТ-инфраструктуры и технологий строить связанные модели, целостность и актуальность которых поддерживается с использованием инвентарных данных об информационных активах.



Предлагаемые решения дают возможность производить сбор аппаратной и программной инвентарной информации с рабочих станций пользователей, сетевых устройств и серверных платформ. Накопленная информация размещается в **централизованной базе данных** конфигурационных единиц и становится доступной для использования всем заинтересованным сторонам. Решения содержат **широкий набор отчетов**, сигнализирующих о необходимости обновления, замены или расширения числа объектов ИТ-инфраструктуры и позволяющих получить максимально **полную** и достоверную **информацию об информационных активах в любой момент времени**.

Предлагаемые решения **подходят для работы в неоднородных и территориально распределенных сетях**. Информация, собираемая в удаленных офисах, может направляться на центральный сервер по протоколу HTTP/HTTPS непосредственно с объекта инвентаризации или накапливаться локально для дальнейшей пересылки.

Автоматический сбор данных может проводиться как путем установки агентов на различные операционные системы класса MS Windows, Mac OS, Linux, UNIX, так и без участия агентов с возможностью разового запуска. Сбор данных о сетевых устройствах осуществляется по SNMP-протоколу с применением баз **Management Information Base (MIB)**. Также возможен ручной ввод информации с использованием веб-интерфейса.

Предлагаемые технические решения поддерживают **широкие возможности для интеграции с другими системами** и могут использоваться как единые централизованные хранилища данных об имеющихся информационных активах (CMDB). Инвентаризация ПО способствует решению задачи обеспечения лицензионной чистоты организации и высвобождения средств, расходуемых на неиспользуемые приложения. Предлагаемые решения позволяют оценить количество установок разнообразных программ, а также частоту их использования на конечных станциях. Дополнительно решение обеспечивает **поиск нежелательных установок приложений и блокировку возможности их запуска**.

Еще одной из задач, решаемой инвентаризацией, является **возможность контроля версий используемого ПО** для ведения процесса управления обновлениями.

Altiris Inventory Solution позволяет получить подробные данные о распространенных программно-аппаратных платформах. Серверная версия решения имеет специальные компоненты для расширенной отчетности по серверному ПО и оборудованию ведущих производителей. Для решения нестандартных задач по сбору данных возможно проведение так называемой кастомизированной инвентаризации, что позволяет расширить функциональные возможности.

Получение целостной картины расположения информационных активов в орг. структуре компании и взаимосвязей между собой и «хозяевами» предлагается **Altiris Asset Management Suite**. Дополнительно к этому этот набор решений позволяет вести **финансовый учет ИТ-активов**.

Сбор информации с конечных станций может осуществляться как с применением агента по заданному расписанию, так и без участия агента с возможностью разового запуска. Также возможен сбор данных со станций, не подключенных к корпоративной сети с помощью внешних перезаписываемых носителей, например flash USB-носителя. Данные, накопленные в базе данных, хранятся в течение заданного периода и позволяют **фиксировать запланированные и несанкционированные изменения** в конфигурации объектов ИТ-инфраструктуры.

Такой подход делает ИТ-инфраструктуру более контролируемой и значительно упрощает процесс аудита.

Построение системы управления уязвимостями

Используемые технические решения:

- Qualys
- Outpost24
- Positive Technologies MaxPatrol
- Symantec CMS/SMS
- Symantec Workflow

Наиважнейшей составляющей процесса обеспечения информационной безопасности является идентификация областей потенциального риска.

Уязвимости основных компонент корпоративной сети: сетевых сервисов, операционных систем, прикладного программного обеспечения, систем управления базами данных, маршрутизаторов, межсетевых экранов — являются фундаментальным риском в процессе обеспечения информационной безопасности.



Оценка защищенности ресурсов сети (сканирование уязвимостей) и последующее устранение обнаруженных уязвимостей **значительно повышает общий уровень безопасности корпоративной ИТ-инфраструктуры**, обеспечивая организации **эффективное управление потенциальными рисками ИБ** и проверку информационной системы на соответствие регламентам (техническим стандартам, законам и подзаконным актам) и внутренним политикам в сфере ИБ.

В качестве технического средства оценки защищенности ресурсов сети используются решения, основанные на **технологии Software-as-a-Service** (ПО как услуга). Это позволяет избежать сложного процесса внедрения и настройки дополнительных элементов инфраструктуры и **избавляет от закупки дополнительного аппаратного обеспечения** и затрат на ее сопровождение.

Компания LETA в рамках услуги «Оценка защищенности ресурсов сети» предлагает два варианта внедрения и выполнения работ:

Разовая оценка защищенности

Специалисты компании LETA с помощью выбранного Заказчиком технического средства выполняют разовое сканирование корпоративной сети согласно заданным параметрам.

По итогам работы подготавливается отчет о результатах сканирования, который содержит описание проведенных работ по выявлению уязвимостей корпоративной сети Заказчика, а также экспертные заключения специалистов LETA и рекомендации по итогам сканирования.

Внедрение системы управления уязвимостями

Специалисты Исполнителя обеспечивают внедрение системы управления уязвимостями на стороне Заказчика, что позволяет значительно повысить защищенность всей информационной системы в целом и вывести ИБ в организации на качественно новый уровень.

Система управления уязвимостями позволяет:

- автоматизировать управление жизненным циклом уязвимостей;
- регламентировать процессы обнаружения, анализа и устранения уязвимостей;
- обеспечить четкий алгоритм устранения обнаруженных в результате сканирования уязвимостей, в приоритетном порядке на основе критичности тех или иных обнаруженных уязвимостей;
- поддерживать в актуальном состоянии высокую степень защищенности корпоративной сети.

В общем случае **состав** внедряемой специалистами LETA **системы управления уязвимостями** выглядит следующим образом:

- **решение по управлению уязвимостями**
сканирование внешних и внутренних ip-адресов корпоративной сети, выявление уязвимостей, их анализ и устранение;
- **соответствие политикам безопасности**
автоматическая проверка на соответствие требованиям политик безопасности, рекомендаций и стандартов (PCI DSS, COBIT, ISO, SOX, Basel II и др.);
- **контроль защищенности веб-приложений**
выявление, анализ и устранение уязвимостей, присущих именно веб-приложениям (SQL-injection, XSS и др.);
- **организационно-распорядительная документация**
набор документов, обеспечивающих регламентирование процесса управления уязвимостями в рамках корпоративной сети, в общем случае включает в себя политику управления уязвимостями, процедуры проведения сканирований и устранения уязвимостей, а также различные инструкции и другие документы.

Программный комплекс **Symantec CMS/SMS** и **Symantec Workflow** предлагается в качестве основы для устранения уязвимостей на конечных объектах корпоративной сети – ПК, ноутбуки и серверные решения. Используемые технологии позволяют решать удаленно и в кратчайшие сроки задачи управления обновлениями и конфигурирования систем с возможностью последующей проверки результата.

Построение системы сбора, корреляции событий и управления инцидентами информационной безопасности

Используемые технические решения:

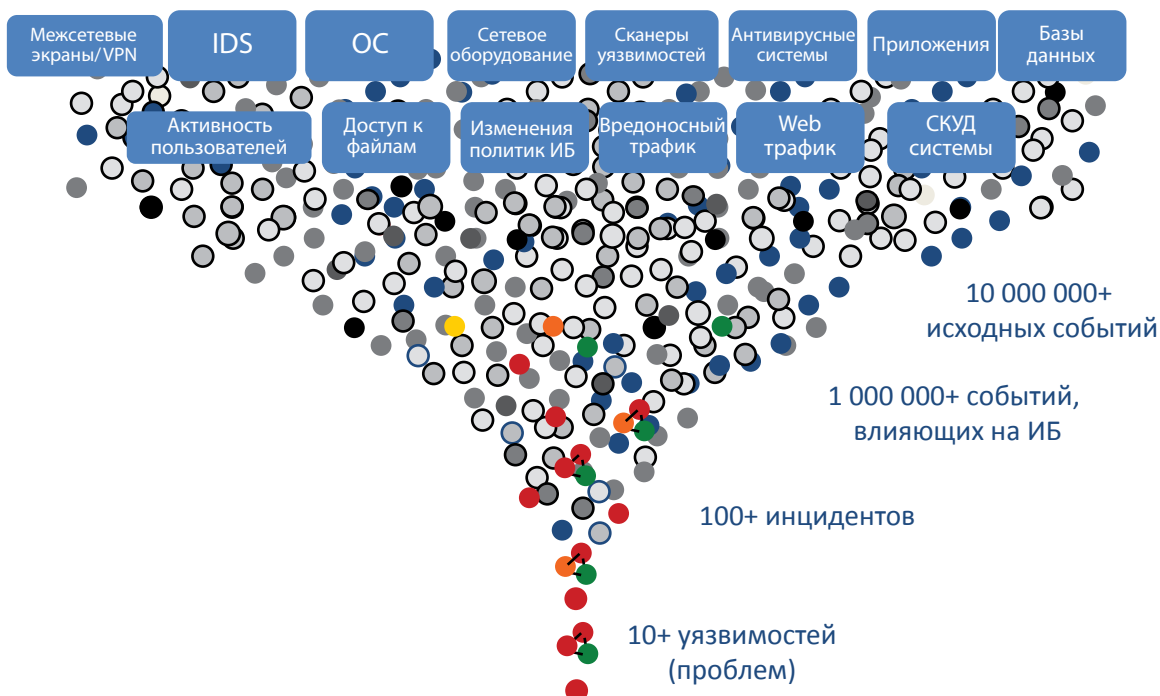
- Symantec Security Information Manager
- Symantec Altiris Service Desk
- Symantec Workflow

Важнейшим фактором для успешного обеспечения информационной безопасности является поступление **полной и своевременной информации о событиях**, происходящих в информационной системе организации.

Анализ этой информации позволяет **выявить инциденты** и проблемы информационной безопасности, которые потенциально могут нанести ущерб организации.

Также для организаций является чрезвычайно важным **наличие процедур анализа и устранения последствий инцидентов**, своевременного расследования причин их возникновения и принятия корректирующих мер для снижения вероятности повторения подобных инцидентов в будущем.

В крупных территориально распределенных организациях количество и разнообразие событий, связанных с информационной безопасностью, настолько велико, что становится невозможным собирать и анализировать их вручную. В результате события, свидетельствующие об инцидентах ИБ, зачастую оказываются незамеченными среди потока других событий.



В то же время по инцидентам, которые все-таки удалось выявить, часто отсутствуют **четкие процедуры реагирования**, расследования и принятия решений о корректирующих мерах.

В результате в системе обеспечения информационной безопасности долгое время **остаются незамеченными серьезные уязвимости**, наличие которых значительно увеличивает финансовые, правовые и репутационные риски организации.

LETA IT-company предлагает специализированное решение, которое представляет собой **совокупность организационных и технических мер**, направленных на достижение следующих результатов:

- оценка уровня безопасности информационной системы;
- оценка эффективности имеющихся мер ИБ;
- сбор и долговременное хранение информации о событиях ИБ с возможностью их последующего анализа;
- реализация эффективных процедур управления инцидентами ИБ: информирование, категорирование, реагирование, локализация, устранение последствий, расследование, принятие корректирующих мер;
- построение гибкой системы отчетности: от отчетов стратегического уровня для руководства до подробных отчетов о конкретных событиях ИБ;
- соблюдение требований ИБ в части мониторинга событий и управления инцидентами.

В рамках проекта по реализации **системы сбора и корреляции событий ИБ и управления инцидентами** могут выполняться следующие **основные задачи**:

- определение области контроля и выбор источников информации о событиях ИБ на основе анализа рисков и актуальных требований;
- разработка и внедрение процедур управления инцидентами;
- проектирование и внедрение программно-технических средств;
- консультационное сопровождение и техническая поддержка.

Программный комплекс **Symantec Security Information Manager (SSIM)**, используемый в качестве основы предлагаемого решения, является модульным продуктом, позволяющим собирать и анализировать события ИБ, выявлять среди них подозрительные и ранжировать их по уровню критичности.

SSIM собирает и хранит данные журналов из множества источников **в центральном хранилище данных** об инцидентах. Приоритеты событий и инцидентов расставляются с учетом важности информационных ресурсов и критичности обнаруженных инцидентов.

Сопоставление с данными, собранными в глобальной сети (в рамках услуги **Symantec «Global Intelligence Network»**), позволяет выделить значимые инциденты среди большого числа зафиксированных событий.

Основные функции, реализуемые SSIM:

- сбор событий ИБ;
- хранение событий, поступающих в систему;
- хранение журналов и механизмы извлечения;
- анализ угроз в режиме реального времени;
- корреляция событий и формирование на их основе инцидентов;
- определение приоритетов инцидентов;
- автоматизация контроля над процессом исправления инцидентов;
- создание отчетов о соблюдении нормативных требований.

Программные продукты **Altiris Service Desk** и **Symantec Workflow** могут использоваться для автоматизации действий сотрудников, участвующих в процессе управления инцидентами на различных его этапах, а также для интеграции предлагаемого решения с программными продуктами, имеющимися у Заказчика.

Построение системы внутреннего аудита и обеспечения соответствия требованиям

Используемые технические решения:

- Symantec Control Compliance Suite
- Positive Technologies MaxPatrol
- ARIS Risk Management & Compliance

Важнейшим фактором для успешного обеспечения информационной безопасности является **наличие в организации четких внутренних требований** в отношении используемых мер и средств ИБ, а также наличие **эффективного контроля за выполнением** этих требований.

К современным организациям также предъявляются различные **требования со стороны законодательства, регулирующих органов и органов по сертификации**. Невыполнение этих требований несет в себе значительные финансовые, правовые и репутационные **риски**.

Такие требования содержатся в:

- Законе №-152 ФЗ «О персональных данных»;
- стандарте международных платежных систем PCI DSS;
- стандарте Банка России СТО БР ИББС;
- международном стандарте ISO IEC 27001:2005;
- стандартах SOX и COBIT.

Обеспечение выполнения внутренних и внешних требований, а также оценка эффективности имеющихся мер контроля являются основными задачами процесса внутреннего аудита ИБ.

LETA IT-company предлагает набор услуг, направленных на **формирование четких требований ИБ** в организации и успешное **обеспечение контроля за их выполнением**.

В соответствующий набор услуг входят:

- оценка соответствия информационной системы Заказчика установленным внешним или внутренним требованиям;
- разработка политик и стандартов в области ИБ;
- разработка и внедрение процедур внутреннего аудита ИБ:
 - о сбор и анализ информации;
 - о определение актуальных требований;
 - о оценка рисков;
 - о оценка эффективности имеющихся мер контроля;
 - о анализ со стороны руководства;
 - о внедрение корректирующих мер по итогам аудита;
- проектирование и внедрение программно-технических средств аудита и контроля за соответствием требованиям;
- разработка технических проверок для информационных систем Заказчика;
- консультационное сопровождение и техническая поддержка.

Предлагаемые программно-технические решения позволяют значительно снизить трудозатраты на выполнение процедур внутреннего аудита ИБ за счет автоматизации процесса, а также существенно повысить полноту и качество собираемой информации.



Рассматриваемые программно-технические средства обеспечивают:

- автоматизацию процесса разработки и пересмотра политик безопасности Компании с учетом внутренних требований и действующих регулятивных норм в области информационной безопасности;
- выполнение технических проверок (настроек, конфигураций приложений, серверов и рабочих станций) в соответствии с установленными политиками и процессами;
- проведение опросов ответственных сотрудников по вопросам, не проверяемым техническими методами, анализ и хранение результатов проверок и сопроводительных документов;
- построение актуальной отчетности о соответствии требованиям на основании сопоставления результатов проверок и принятых требований/стандартов безопасности;
- управление задачами для всех сотрудников, задействованных в процессе внутреннего аудита на различных этапах.

Построение системы управления информационными рисками

С увеличением зависимости компаний от используемых информационных технологий растут связанные с ними риски. К таким рискам относятся внутреннее и внешнее мошенничество, несанкционированное использование ресурсов Компании, нарушение конфиденциальности информации, ошибки персонала, сбои информационных систем, несоответствие требованиям законодательства и многие другие.

Выявление и снижение информационных рисков - основная бизнес-задача для службы информационной безопасности. И чем сложнее становятся автоматизированные системы и процессы обработки информации, тем труднее эту задачу решать.

Для организации эффективного управления информационными рисками **компания LETA предлагает** услугу по построению комплексной системы, которая позволит:

- обеспечить своевременное выявление и решение проблем безопасности;
- снизить количество случаев непредвиденных потерь;
- согласовать цели информационной безопасности с целями бизнеса;
- значительно повысить прозрачность деятельности службы ИБ для руководства;
- повысить уровень капитализации Компании;
- оптимизировать затраты на реализацию мер по обеспечению ИБ.

Процедуры управления рисками строятся в соответствии с лучшими современными практиками и требованиями регуляторов (**COSO, BASEL II, положения Банка России** и т.п.), могут быть интегрированы с корпоративной системой управления операционными рисками и автоматизированы с помощью специализированных программных решений. Система управления информационными рисками подразумевает непрерывный циклический процесс и включает набор взаимосвязанных процедур.



Внедрение системы управления рисками ИБ, как правило, проводится поэтапно. Каждый из этапов ограничен по времени и **приносит Компании ощутимый результат**. Методика внедрения предполагает передачу сотрудникам Заказчика необходимых знаний и опыта для того, чтобы впоследствии они могли сами поддерживать и развивать систему управления информационными рисками в Компании.

Проект по внедрению системы управления рисками ИБ включает следующие этапы:

- выбор области деятельности, в которой будет выполняться проект;
- разработку методологии управления информационными рисками;
- проведение оценки рисков в соответствии с разработанной методологией в выбранной области;
- внедрение средств автоматизации процедур управления рисками ИБ и их тестовую эксплуатацию;
- обучение сотрудников Заказчика разработанной методологии и средствам автоматизации;
- информационную поддержку Заказчика в процессе использования внедренной системы.

По окончании реализации проекта **организация получает эффективную систему управления**, направленную на снижение информационных рисков и достижение целей бизнеса.

Построение системы обеспечения непрерывности бизнес-процессов

Современные организации в своей работе сталкиваются с объективными факторами:

- усилением конкуренции;
- повышением сложности и критичности используемых информационных систем;
- увеличением зависимости важных процессов от внешних поставщиков услуг;
- ростом угроз, связанных с чрезвычайными ситуациями: техногенными, природными, социальными;
- принятием российскими регулирующими органами и международными организациями нормативных актов, касающихся обеспечения непрерывности деятельности.

Все эти факторы делают задачу построения системы обеспечения непрерывности деятельности крайне важной для современных кредитно-финансовых организаций и вынуждают банки приступить к целенаправленному и планомерному ее решению.

Система обеспечения непрерывности деятельности представляет собой комплекс мер, обеспечивающих непрерывность (устойчивость) функционирования банка в чрезвычайных ситуациях, в том числе защиту объектов и персонала банка от ЧС, а также непрерывность критических процессов банковской деятельности.

При построении системы обеспечения непрерывности деятельности организации могут руководствоваться следующими нормативными документами:

- Британским стандартом BS 25999, содержащим лучшие мировые практики по обеспечению непрерывности деятельности;
- Указанием ЦБ РФ №2194-У «О внесении изменений в положение Банка России от 16 декабря 2003 года №242-П. «Об организации внутреннего контроля в кредитных организациях и банковских группах», включающим рекомендации по обеспечению непрерывности деятельности в организациях Банковской системы РФ;
- Положениями Базельского комитета, включающими задачу управления непрерывностью деятельности как одну из задач управления операционными рисками

LETA IT-компану оказываает своим Клиентам следующие услуги в области обеспечения непрерывности деятельности:

Разработка стратегии непрерывности деятельности

Услуга по разработке стратегии непрерывности деятельности позволяет идентифицировать критичные бизнес-процессы и области деятельности и спланировать меры по обеспечению их непрерывности.

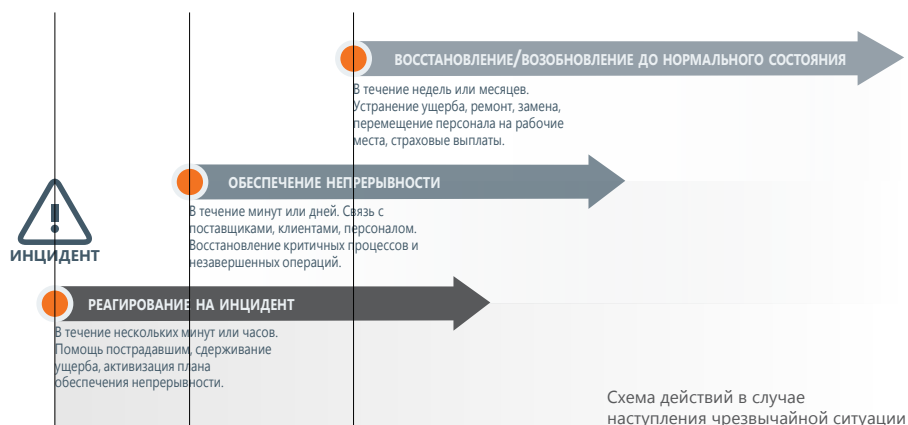
В рамках данной услуги производится:

- идентификация критически важных для организации процессов и поддерживающих их ресурсов;
- оценка возможного ущерба от нарушения критичных процессов в случае чрезвычайных ситуаций;
- оценка рисков нарушения непрерывности бизнеса;
- определение требований непрерывности;
- выбор общих способов обеспечения непрерывности для критически важных бизнес-процессов на основе технического и финансового анализа;
- разработка стратегии обеспечения непрерывности бизнеса организации, определяющей общие подходы к созданию системы обеспечения непрерывности деятельности и описывающей программу ее создания.

Разработка и внедрение мер по обеспечению непрерывности деятельности

Данная услуга предполагает разработку и внедрение мер по обеспечению непрерывности деятельности в соответствии с выбранной стратегией.

- описание критичных бизнес-процессов, выбор оптимальных способов восстановления для каждого из них;
- внедрение катастрофоустойчивых решений;
- разработка планов разрешения инцидентов (IMP), обеспечения непрерывности бизнеса (BCP) и планов восстановления деятельности (DRP);
- обучение персонала;
- тестирование разработанных планов.



В рамках данной услуги в случае необходимости может осуществляться внедрение технических средств обеспечения непрерывности функционирования ИТ-инфраструктуры и катастрофоустойчивых решений.

В рамках данной услуги может проводиться построение катастрофоустойчивой ИТ инфраструктуры, необходимой для выполнения соответствующих планов.

Дополнительно может быть произведено внедрение прикладных систем для автоматизации работ с планами обеспечения непрерывности деятельности (НБ).

Разработка и внедрение системы управления НБ на основе стандарта BS25999-2

Услуга предполагает внедрение системы управления непрерывностью бизнеса на основе рекомендаций стандарта BS25999-2, которая позволит организации управлять изменениями и поддерживать планы обеспечения непрерывности бизнеса в актуальном состоянии.

В рамках услуги в случае необходимости могут быть внедрены прикладные системы для автоматизации процессов управления непрерывностью деятельности.

Подготовка системы управления непрерывностью деятельности к сертификации в соответствии с требованиями стандарта BS25999-2

Услуга предлагается организациям, преследующим цели получения сертификата соответствия стандарту BS25999-2 для демонстрации заинтересованным сторонам, и подразумевает проведение двух основных этапов работ:

- На **первом этапе** подготовки к сертификации проводится **обследование и анализ выполнения требований стандарта BS25999-2**, разрабатываются рекомендации по устранению выявленных несоответствий.
- **Второй этап** подготовки к сертификации включает **проведение предварительного аудита** и устранение выявленных несоответствий.
- **Третий этап – сертификационный аудит**, проводится независимым сертификационным органом. В процессе проведения сертификационного аудита LETA IT-company осуществляет информационную поддержку клиента.

Услуги и решения
LETA IT-company в
области
соответствия
требованиям

Обеспечение соответствия требованиям Федерального закона РФ № 152-ФЗ «О персональных данных»

26 января 2007 г. вступил в силу Федеральный закон № 152-ФЗ «О персональных данных», который определил необходимость защиты персональных данных (ПДн) субъектов.

Информационные системы, обрабатывающие ПДн, должны быть приведены в соответствие с требованиями Федерального закона не позднее 1 января 2010 года. Согласно принятому законопроекту «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных» данный срок перенесен на 1 год – до 1 января 2011 года.

За невыполнение требований Закона «О персональных данных» предусмотрена административная и уголовная (в соответствии со статьями КоАП и УК РФ) ответственность. Ответственность может быть наложена как на юридические (организации), так и на физические лица: рядовых сотрудников и руководителей предприятия. Деятельность организации по обработке ПДн также может быть приостановлена по требованию Роскомнадзора.

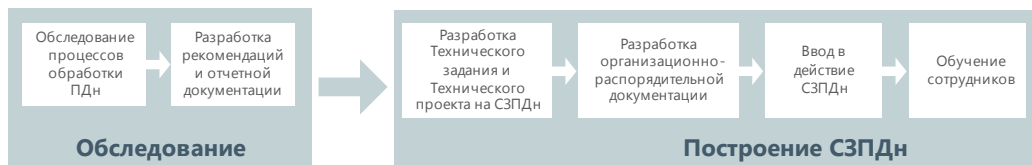
Услуги по защите ПДн направлены на снижение рисков карательных санкций со стороны регулирующих органов, определенных в законе: ФСБ России, ФСТЭК России и Роскомнадзора.

Построение системы защиты персональных данных (СЗПДн) от LETA IT-компании позволяет решить следующие задачи:

- документирование процессов обработки ПДн, обрабатываемых в организации;
- категорирование ПДн и составление перечня подразделений, допущенных к обработке ПДн;
- обоснование классификации информационных систем, обрабатывающих ПДн;
- анализ существующих организационных и технических мер по обеспечению безопасности ПДн;
- разработка моделей угроз безопасности ПДн при их обработке в информационных системах персональных данных (ИСПДн);
- обоснование классификации ИСПДн;
- разработка рекомендаций и мероприятий по приведению процессов обработки ПДн организации в соответствие с требованиями законодательства РФ;
- формирование требований к построению СЗПДн (разработка Технического задания и Технического проекта на создание СЗПДн);
- устранение выявленных в организации несоответствий требованиям законодательства и руководящих документов регулирующих органов (поставка и внедрение необходимых средств защиты информации, разработка организационно-распорядительной документации);
- подтверждение соответствия процессов обработки ПДн требованиям Закона № 152-ФЗ (декларирование соответствия требованиям по безопасности информации/аттестация ИСПДн по требованиям безопасности информации).

Услуги LETA IT-компану в области защиты персональных данных

Основной блок услуг LETA IT-компану по построению систем защиты персональных данных



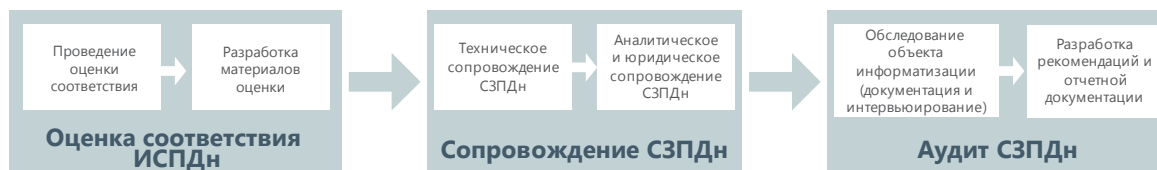
Обследование системы персональных данных на соответствие требованиям Федерального закона РФ № 152-ФЗ «О персональных данных»

- документирование процессов обработки ПДн;
- определение и исследование информационных систем обработки ПДн;
- разработка документации, необходимой либо рекомендуемой руководящими документами ФСТЭК России и ФСБ России (Модели угроз безопасности ПДн, акты классификации ИСПДн, Технические паспорта ИСПДн, Перечень ПДн, обрабатываемых в организации, Перечень ИСПДн, Перечень подразделений и сотрудников, допущенных к обработке ПДн, и др.);
- разработка рекомендаций по приведению процессов обработки ПДн в соответствие с требованиями законодательства РФ.

Построение системы защиты персональных данных в соответствии с требованиями Закона № 152-ФЗ «О персональных данных»

- проектирование СЗПДн (разработка Технического задания, Технического проекта и др.) в соответствии с требованиями руководящих документов;
- поставка и установка необходимых средств защиты информации, перевод СЗПДн в промышленную эксплуатацию;
- разработка необходимой организационно-распорядительной документации;
- обучение сотрудников организации работе с компонентами СЗПДн;
- подготовка материалов для получения организацией лицензий ФСТЭК России и ФСБ России (при необходимости).

Дополнительный блок услуг LETA IT-компану



Оценка соответствия информационной системы персональных данных требованиям Закона № 152-ФЗ «О персональных данных»

- проведение оценки соответствия средств защиты требованиям руководящих документов;
- разработка материалов оценки соответствия (протоколы, заключения).

В соответствии с приказом ФСТЭК России от 05 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», а также в соответствии с Решением ФСТЭК России от 05 марта 2010 г. аттестация ИСПДн более не является обязательной.

Сопровождение системы защиты персональных данных в соответствии с требованиями Закона № 152-ФЗ «О персональных данных»

- консультации Заказчика по техническим вопросам, установка и настройка новых компонентов СЗПДн;
- консультации Заказчика в случае изменения структуры и состава ИСПДн;
- доработка организационно-распорядительной документации в случае необходимости.

Аудит системы защиты персональных данных на соответствие требованиям Закона № 152-ФЗ «О персональных данных»

- проведение аудита построенной СЗПДн на соответствие требованиям законодательства РФ;
- разработка отчета, описывающего выявленные несоответствия и рекомендации по их устранению.

Подход LETA IT-компании к оказанию услуг в области защиты персональных данных в соответствии с требованиями Закона № 152-ФЗ «О персональных данных»

Снятие рисков применения карательных санкций со стороны регулирующих органов (ФСБ России, ФСТЭК России, Роскомнадзора)

Все работы выполняются в соответствии с федеральным законодательством, подзаконными актами и нормативными документами, регулирующими вопросы защиты персональных данных.

Поддержание работы бизнес-процессов компании

LETA стремится сохранить в целостности основные бизнес-процессы компании Заказчика, обеспечив при этом выполнение необходимых требований РД регулирующих органов.

Снижение затрат оператора на внедрение решений по защите персональных данных

Решения LETA по защите персональных данных направлены на нахождение разумного баланса, обеспечивающего выполнение как необходимых требований регулирующих органов, так и требований бизнеса.

Обеспечение соответствия требованиям PCI DSS

Построение системы ИБ в соответствии с требованиями PCI DSS позволяет внедрить необходимые механизмы защиты данных о держателях пластиковых карт, обеспечивающие выполнение требований международного стандарта безопасности в области платежной индустрии PCI DSS (Payment Card Industry Data Security Standard). Соответствие стандарту позволяет организации достичь максимального уровня безопасности при всех операциях, связанных с платежными картами.

Действие PCI DSS распространяется на все торгово-сервисные предприятия и поставщиков услуг, работающих с международными платежными системами, т.е. на всех тех, кто передает, обрабатывает и хранит данные держателей карт. Стандарт поддерживается такими международными платежными системами, как Visa® International, MasterCard® Worldwide, American Express®, JCB® и Discover® Financial Services.

Построение системы информационной безопасности в соответствии с требованиями PCI DSS обеспечивает Заказчику:

- соответствие механизмов защиты данных о держателях пластиковых карт рекомендациям PCI DSS;
- повышение защиты критичных бизнес-процессов и информационных ресурсов;
- повышение доверия со стороны партнеров, клиентов, инвесторов.

Перед построением системы информационной безопасности в соответствии с требованиями PCI DSS, как правило, проводится оценка защищенности среды данных платежных карт, выявляются несоответствия требованиям PCI DSS, определяется перечень мер по их устранению. Эти работы также могут быть выполнены сторонней организацией, обладающей необходимой квалификацией, а также, как показывает практика, статусом Qualified Security Assessment (QSA) PCI DSS.

По аналогии с аудитом на соответствие требованиям PCI DSS построение надлежащей системы ИБ проводится по следующим направлениям:

- оценка рисков (идентификация угроз и уязвимостей с результатами в виде формализованной оценки рисков безопасности среды данных платежных карт);
- разработка необходимого комплекта документации (документальное оформление и адаптация под индивидуальные особенности Заказчика политик, конфигурационных стандартов и процедур информационной безопасности);
- внедрение необходимых средств защиты информации;
- консультирование специалистов Заказчика (вопросы организации и проведения мероприятий, направленных на повышение квалификации сотрудников Заказчика в сфере обеспечения ИБ).

Результаты работ документируются и по окончании проекта передаются Заказчику в виде отчета.

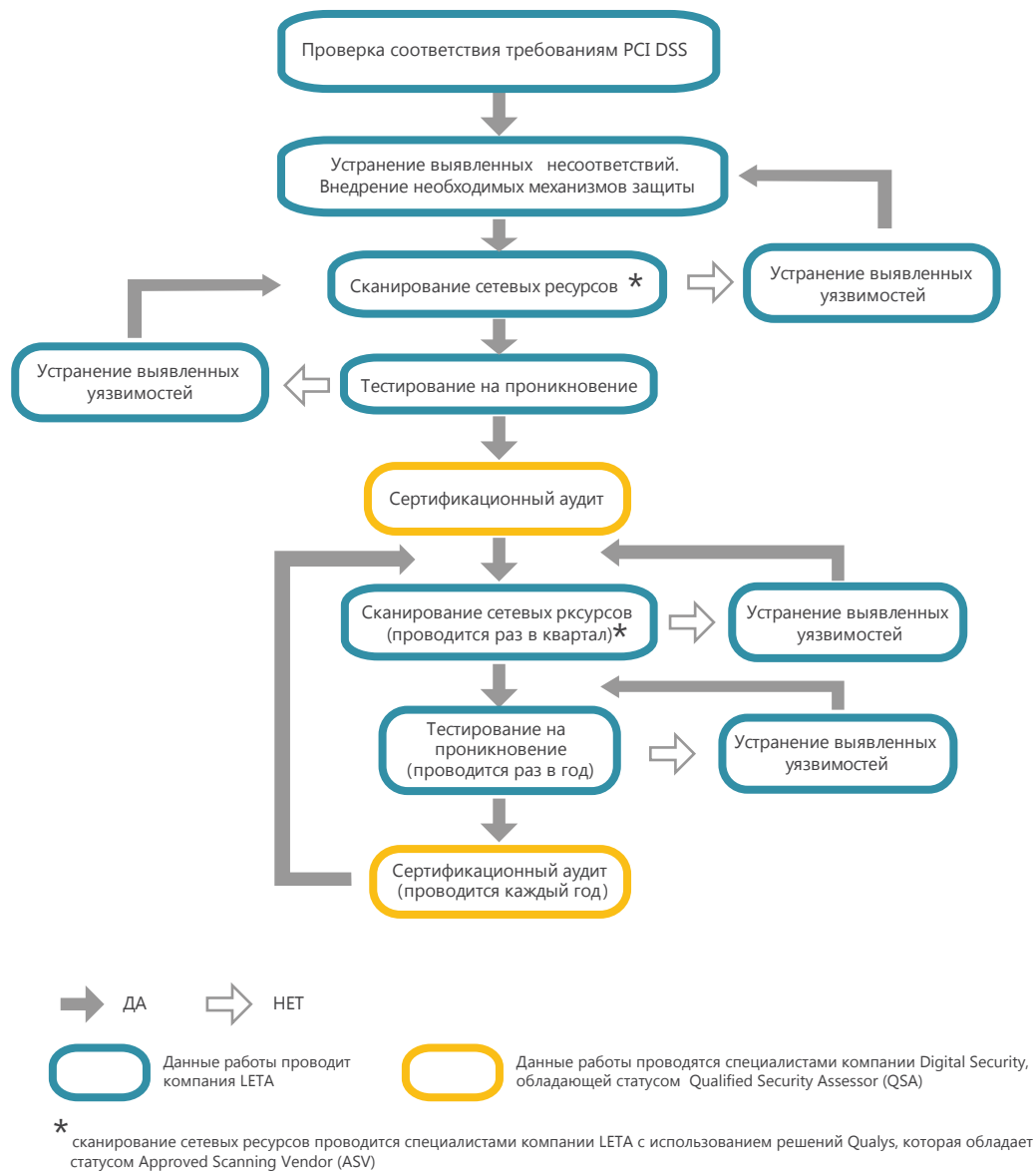


Рисунок. Участие LETA в классическом алгоритме работ по PCI DSS.

Обеспечение соответствия требованиям СТО БР ИББС

Услуга по построению системы менеджмента ИБ в соответствии с требованиями СТО БР ИББС ориентирована на организации банковской сферы и обеспечивает создание системы управления информационной безопасностью, учитывающей лучшие мировые практики менеджмента ИБ, а также отраслевую специфику российских банковских организаций.

В 2004 г. Банк России в целях повышения уровня информационной безопасности организаций банковской системы РФ издал стандарт СТО БР ИББС-1.0-2004 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Стандарт определил необходимые требования к принципам и уровню организации ИБ в кредитно-финансовых учреждениях. Стандарты серии СТО БР ИББС рекомендуются Банком России для применения в учреждениях банковской системы РФ.

Построение системы менеджмента информационной безопасности от LETA IT-company в соответствии с требованиями СТО БР ИББС 1.0 обеспечивает:

- снижение рисков ИБ и повышение эффективности мероприятий по обеспечению ИБ;
- повышение защиты критичных бизнес-процессов и информационных ресурсов Заказчика;
- создание основы для реализации требований законодательства и других международных стандартов по ИБ;
- подтверждение приверженности организации рекомендуемым требованиям регулятора банковской отрасли РФ – Банка России;
- повышение доверия к организации со стороны партнеров, клиентов, акционеров.

В рамках услуги по построению системы менеджмента ИБ в соответствии с требованиями СТО БР ИББС специалисты LETA IT-company:

- **проводят предварительный внешний аудит;**
Эффективное планирование проекта по внедрению требований СТО БР ИББС 1.0 должно основываться на объективных оценках несоответствий ИБ организации положениям стандарта;
- **разрабатывают стратегии и планы поэтапного выстраивания системы менеджмента информационной безопасности;**
Сведения о текущем уровне соответствия, полученные по итогам аудита, позволяют оценить бюджет проекта и общие сроки достижения необходимого уровня соответствия;
- **проводят оценку рисков ИБ;**
Полученные результаты позволяют определить необходимые защитные меры по обработке рисков в отношении ценных информационных активов Заказчика;
- **создают инфраструктуру информационной безопасности (политики, персонал, процессы);**
Эффективное обеспечение ИБ возможно только за счет построения инфраструктуры ИБ, представляющей собой совокупность документированных политик, персонала соответствующих служб, а также организационных процессов по управлению и контролю за ИБ;
- **внедряют необходимые защитные меры.**
Защитные меры организационного и инженерно-технического характера, выбранные на основании результатов оценки рисков ИБ, должны быть установлены, проверены и введены в эксплуатацию.

Одним из результатов внешнего аудита в рамках построения системы менеджмента ИБ в соответствии с требованиями СТО БР ИББС является определение степени выполнения положений стандарта по трем направлениям:

- 1) текущий уровень ИБ организации;
- 2) менеджмент ИБ организации;
- 3) уровень осознания ИБ организации.

Согласно методике, описанной в стандарте, оценка проводится по 32 групповым показателям ИБ. Для более наглядного отображения полученных результатов оценки составляется круговая диаграмма.

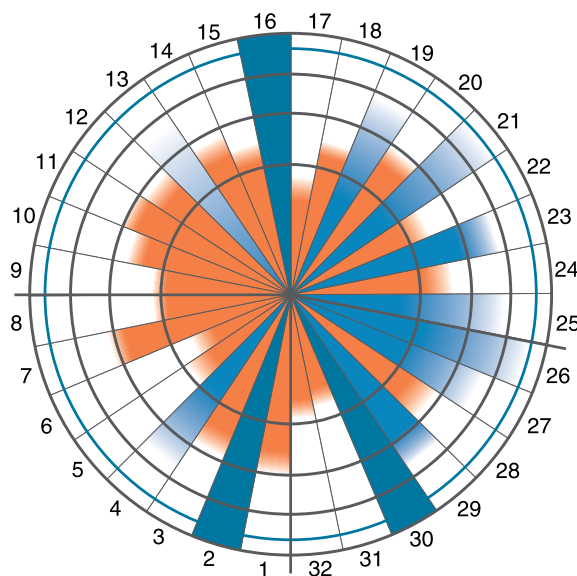


Рисунок. Пример диаграммы результатов оценки уровня ИБ организации

По итогам проведенной оценки уровень ИБ организации может быть отнесен к одному из 5 уровней соответствия по положениям СТО БР ИББС. Банком России рекомендованы уровни 4 и 5.

Полученные сведения о текущем уровне соответствия могут быть использованы менеджментом банковской организации при разработке стратегических планов по повышению уровня соответствия требованиям СТО БР ИББС и определении необходимых для этого затрат.

Услуги и решения
LETA IT-company по
обеспечению
информационной
безопасности

Построение системы противодействия утечке конфиденциальной информации

Используемые технические решения:

- Symantec Data Loss Prevention
- Websense Data Security Suite
- McAfee DLP
- InfoWatch Traffic Monitor, InfoWatch Data Control
- Trend Micro DLP

Системы защиты от утечек данных и инсайдеров (DLP) обеспечивают контроль за распространением конфиденциальной информации за пределы предприятия по всем доступным каналам. DLP-решения (Data Loss, или Leak(age), Prevention) предотвращают несанкционированные операции с конфиденциальной информацией (копирование, изменение и т.д.) и ее перемещение (пересылку, передачу за пределы организации, пересохранение в альтернативные директории и т.д.) через контроль:

- отправки корпоративной и веб-почты (mail.ru, gmail.com и т.п.);
- ftp-соединений;
- передачи мгновенных сообщений (ICQ, MSN, AOL и т.п.);
- печати документов на принтере;
- использования внешних USB-накопителей, CD/DVD, мобильных устройств;
- локальных соединений – Bluetooth, Wi-Fi и т.п.

С развитием технологий увеличивается риск того, что конфиденциальные документы стратегической важности окажутся доступными внешним лицам, причем зачастую не в результате взлома и проникновения, а в результате неосторожных действий и усилий собственных сотрудников компании (инсайдеров). Вступление в силу Федеральных законов № 152-ФЗ «О персональных данных» и № 98-ФЗ «О коммерческой тайне» требует принятия эффективных мер по контролю над доступом и использованием защищаемой информации.

Основные преимущества систем DLP перед альтернативными решениями – продуктами шифрования, разграничения доступа, контроля доступа к сменным носителям, архивирования электронной корреспонденции, статистическими анализаторами – это:

- контроль за всеми каналами передачи конфиденциальной информации в электронном виде (включая локальные и сетевые способы), регулярно используемыми в повседневной деятельности;
- обнаружение защищаемой информации по ее содержанию (независимо от формата хранения, каналов передачи, грифов и языка);
- блокирование утечек (приостановка отправки электронных сообщений или записи на USB-накопители, если эти действия противоречат принятой в Компании политике безопасности);
- автоматизация обработки потоков информации согласно установленным политикам безопасности (внедрение DLP-системы не требует расширения штата службы безопасности).

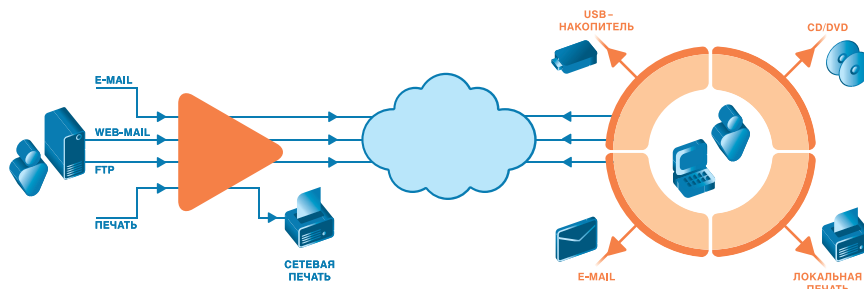


Рисунок. DLP-системы обеспечивают контроль за утечкой информации по сетевым каналам организации и от локальных рабочих станций пользователей

На основе DLP-решений Symantec DLP, Websense DSS, InfoWatch TM, McAfee DLP были построены системы защиты от утечек как в крупных территориально распределенных предприятиях, так и в организациях средних размеров с парком от 250 компьютеров. Небольшие российские компании используют решения McAfee Host DLP и InfoWatch Data Control. Перечисленные решения обеспечивают комплексный контроль за всеми потенциальными путями перемещения конфиденциальной информации.

По итогам внедрения система DLP обеспечивает:

- автоматизированный аудит мест расположения конфиденциальной информации;
- автоматизированный контроль соответствия установленным в Компании процедурам перемещений конфиденциальной информации (создание и обработка инцидентов при неправомерном разглашении секретных сведений с возможностью их предотвращения);
- отслеживание общего уровня рисков (на основе отчетов по инцидентам);
- контроль утечек информации в режиме немедленного реагирования и в рамках ретроспективного анализа;
- приведение уровня информационной безопасности организации в соответствие с рядом требований стандарта PCI DSS и других.

Построение системы контроля устройств ввода-вывода информации

Используемые технические решения:

- McAfee Device Control
- SecurIT Zlock
- SmartLine DeviceLock
- Symantec SEP

Система контроля устройств ввода-вывода информации от LETA IT-company позволяет **предотвратить случайные и преднамеренные случаи несанкционированной передачи корпоративных данных на внешние носители** (через порты и другие каналы обмена информацией) и регламентировать последующее использование устройств ввода-вывода данных в соответствии с нормами информационной безопасности организации.

Сегодня на любом современном компьютере в распоряжении инсайдеров интерфейсы ввода-вывода, обеспечивающие доступ к компактным носителям информации (USB-Flash, CD/DVD диски, ZIP), высокоскоростным беспроводным сетям (Wi-Fi, Bluetooth) и т.д. При отсутствии корпоративных средств контроля за сохранностью информации это позволяет рядовому пользователю даже без использования почтовых ресурсов и выхода в Интернет – при помощи штатных коммуникационных возможностей персонального компьютера – **вынести секретные данные организации за пределы ее информационного периметра**.

В настоящее время практически все предприятия ощущают **необходимость в защите корпоративных данных от утечек**. Основной источник этой угрозы находится внутри организаций. Согласно исследованиям в области информационной безопасности за последние годы, **70–80%** инцидентов нарушения информационной безопасности приходится на так называемые **«внутренние угрозы»** – утечки конфиденциальной информации вследствие неосторожности либо преднамеренных действий сотрудников.

Так как мобильные носители информации получают все более широкое распространение, **контроль устройств ввода-вывода** информации становится одной из наиболее злободневных задач в сфере информационной безопасности.

В рамках построения системы контроля устройств ввода-вывода информации **LETA IT-company обеспечивает Заказчику разработку частной политики ИБ** (включая политику по обращению с периферийными устройствами), а также приложений к ней – **перечня рисков, реестра применяемых средств, структурной схемы защиты, руководств администратора и пользователя системы, процедуры регистрации и обработки инцидентов**.

Для борьбы с утечкой конфиденциальной информации с персональных компьютеров через устройства ввода-вывода **LETA IT-company реализует комплекс решений**, состоящий из:

- **организационных мер** (политики и регламенты безопасности, матрицы пользователей информационных ресурсов и разрешенных к использованию устройств ввода-вывода информации);

- **технических средств** (систем), обеспечивающих:
 - централизованное разграничение доступа к средствам передачи информации (устройствам записи CD-R и DVD-R, портам ввода-вывода, включая USB, беспроводные сети Wi-Fi и Bluetooth);
 - журналирование истории обращения к средствам ввода-вывода;
 - осуществление теневого копирования передаваемой информации;
 - опционально – контроль за содержанием конфиденциальных сведений в передаваемой информации.

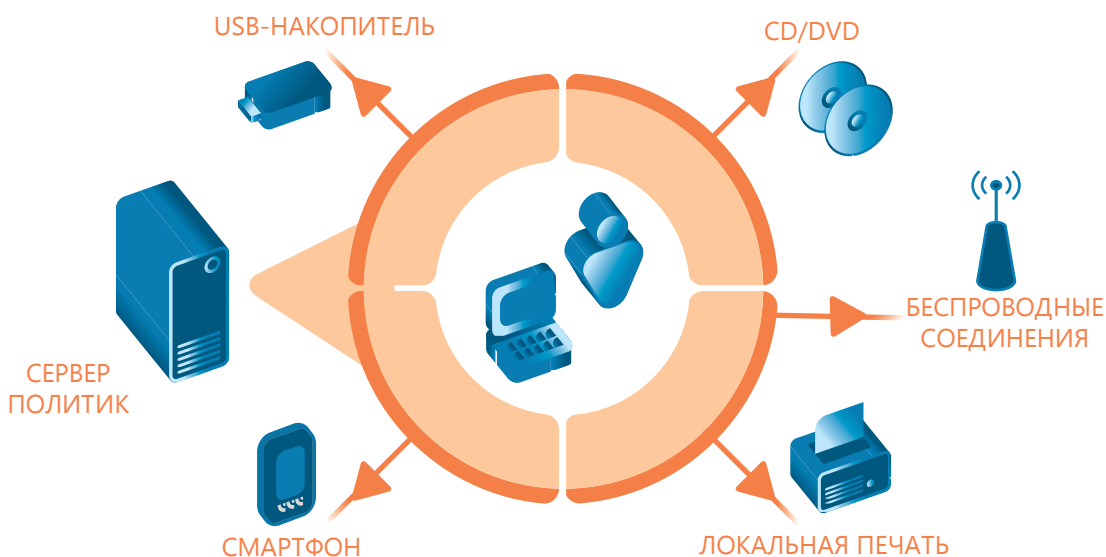


Рисунок. Схема работы системы контроля устройств ввода-вывода

Построенная LETA IT-company **система контроля устройств ввода-вывода** информации **функционирует следующим образом**: агентская программа, рассылаемая через групповые политики на все рабочие места пользователей, отслеживает исполнение политики безопасности по обращению ко всем сменным носителям информации и устройствам, подключаемым к портам ввода-вывода рабочих станций – CD/DVD-накопителям, кард-ридерам, дискетам, ZIP-устройствам, внешним жестким дискам и любым внешним устройствам, подключаемым через порты (USB, PCMCIA, COM, LPT, FireWire, IrDA, Wi-Fi, Bluetooth, устройства печати документов – сетевые и локальные принтеры).

Построение корпоративной системы контроля входящего веб-трафика

Используемые технические решения:

- Websense Web Security
- Aladdin eSafe
- Blue Coat
- McAfee Web Gateway
- Content Keeper
- IBM ISS Proventia
- Symantec Web Gateway
- Microsoft TMG

Система контроля входящего веб-трафика «сканирует» и анализирует поток данных («пакетов»), поступающих по сетевым каналам организации в ответ на запросы пользователей (обращения к сайтам, команды на скачивание файлов и т.д.), на предмет их потенциальной опасности. Система в режиме реального времени (онлайн) изолирует опасный трафик от внутренней сети организации, предотвращая возможные угрозы информационной защиты.

В состав системы контроля входящего веб-трафика от LETA IT-company входят системы веб-фильтрации и веб-безопасности, позволяющие Заказчику:

- снизить издержки на устранение опасных последствий воздействия вредоносного кода в Интернете за счет сокращения соответствующих рисков;
- контролировать рабочее время и эффективность сотрудников, ограничив возможные злоупотребления доступом в Интернет лимитом/запретом на посещение сайтов нерабочей тематики;
- регулировать пропускную способность сети и избегать задержек в коммуникациях в связи с перегрузкой каналов связи в часы пик;
- обеспечить осведомленность руководителей об использовании Интернета сотрудниками организации через исчерпывающую статистику подключений.

По данным Websense, при бесконтрольном доступе в Интернет среднестатистический сотрудник тратит на посещение нерабочих сайтов 6,5 часов в неделю, а 44% сотрудников, по данным Nielsen, в рабочее время активно пользуются ресурсами с аудио-/видеопотоковой информацией.

Система веб-фильтрации представляет собой приложение, содержащее базу с миллионами адресов веб-сайтов, каждому из которых присвоена «репутация» и одна из целевых категорий – например, «новостные», «поисковые порталы», «веб-почта», «социальные сети» и т.п. Обновления базы поступают ежедневно, за их актуальность отвечает разработчик системы.

Система веб-фильтрации устанавливается на выделенный сервер и подключается к корпоративному прокси-серверу (или зеркалирующему порту до прокси-сервера), «копируя» себе проходящий веб-трафик пользователей.

Когда сотрудник запрашивает в браузере какую-либо страницу, система веб-фильтрации фиксирует инициатора и время запроса, запрошенный ресурс, его категорию по базе.

Если запрошенный веб-ресурс принадлежит «черной» категории, система посылает запрос на прокси-сервер об отмене доступа пользователю и выдает ему одно из настроенных действующими политиками уведомлений («Ваша квота на данный ресурс исчерпана», «Вы обратились к сайту категории "Развлекательные ресурсы"» и т.п.).

Преимущества системы веб-фильтрации:

- управление веб-трафиком сотрудников;
- безопасность (отслеживание и предотвращение доступа сотрудников к потенциально опасным ресурсам Интернета);
- контроль протоколов. Система отслеживает не только куда (на какие ресурсы), но и как – по какому протоколу, каким способом (через веб-браузер, ICQ, зашифрованный канал и т.д.) – сотрудники выходят в Интернет;
- управление пропускной способностью и производительностью корпоративного канала доступа в Интернет (приоритет целевого использования ресурсов в случае загруженности корпоративной сети);
- построение отчетов о результатах использования ресурсов Интернета, в том числе статистика и аналитическая отчетность;
- управляемость (распределение ролей администраторов по настройкам политики безопасности, в том числе в распределенной сети).

Для оптимального обоснования необходимости внедрения системы веб-фильтрации по согласованию с Заказчиком специалисты LETA IT-компану проводят «пилотное» внедрение системы, позволяющее оценить ее эффективность в реальных условиях бизнеса клиента.

В рамках проекта по построению системы контроля входящего веб-трафика специалисты LETA IT-компану не только проводят внедрение системы, но и разрабатывают инструкционные (эксплуатационные) документы, готовят политики безопасности, создают матрицы доступа.

Websense Web Security представляет собой передовое решение фильтрации веб-трафика, повышающее производительность сотрудников, оптимизирующее использование ресурсов Интернета, позволяющее управлять пропускной способностью сети. Это решение сочетает не только передовые возможности **url-фильтрации**, но и обладает широким набором средств веб-безопасности. Оно включает в себя службы веб-репутации и полный набор url-категорий безопасности: бот сети, шпионские программы, фишинг и мошенничество, перехватчики клавиатуры, вредоносные веб-сайты, потенциально нежелательные программы. Продукт обеспечивает **контроль над системами обмена мгновенными сообщениями**. Благодаря интуитивно понятному веб-интерфейсу легко настраиваются политики использования Интернета сотрудниками. Решение не только управляет доступом к сайтам, но и **контролирует более 100 сетевых протоколов**, обладает высокой масштабируемостью и интегрируется с широким кругом сторонних сетевых устройств.

Комплекс решений **eSafe** предназначен для обеспечения **многоуровневой системы превентивной защиты** информации в корпоративных сетях. eSafe позволяет **регулировать время пребывания пользователей в сети Интернет и блокировать их доступ к неразрешенным ресурсам**. Это решение обеспечивает комплексную и гибкую защиту трафика, передающегося по протоколам HTTP и FTP, предназначено для борьбы с вирусами, шпионскими программами и осуществления функции фильтрации URL, а также реализации политик безопасности, принятых в компании. Позволяет проводить инспекцию трафика «на лету», благодаря использованию технологии NitroInspection. **Централизованная система управления eConsole** дает возможность администратору осуществлять удаленное конфигурирование системы и управление всеми компонентами eSafe, установленными в сети.

Семейство устройств **Blue Coat ProxySG** представляет собой архитектуру масштабируемых платформ прокси для обеспечения безопасности веб-коммуникаций и ускорения доставки бизнес-приложений. Устройство позволяет обеспечить безопасность веб-коммуникаций путем блокировки программ-шпионов, вирусов и других нежелательных данных, управлять доступом по пользователям и приложениям, обеспечивая соблюдение правил доступа в Интернет, ускорять передачу данных через Интернет или WAN (глобальные сети) с помощью интегрированных систем кэширования и сжатия данных. Оно может быть дополнено устройством **Proxy AV** – антивирусом, который позволит организациям обнаруживать вирусы, черви, шпионские программы и трояны на интернет-шлюзе. Proxy AV способен блокировать большую часть неизвестных шпионских программ, атакующих через HTTP-, FTP- и HTTPS- протоколы. **Blue Coat WebFilter** позволяет фильтровать интернет-трафик в соответствии с политиками использования Интернета, принятыми в компании.

ContentKeeper Web - это масштабируемое, отказоустойчивое решение по фильтрации Интернета, позволяющее осуществлять мониторинг, управление, контроль и защиту в процессе использования интернет-ресурсов. Гибкие методы контроля позволяют управлять доступом на уровне сайтов, категорий сайтов, типов файлов, типов медиафайлов, пользователей, групп, сетевых адресов, интервалов времени, SSL, полосы пропускания и целого ряда других параметров. Решение может быть дополнено **ContentKeeper SSLi** и **ContentKeeper Anti-Virus** для работы с шифрованным трафиком и антивирусной защиты.

IBM Proventia Network Multi-Function Security - многофункциональное устройство, объединяющее в себе следующие средства информационной защиты: полноценный межсетевой экран, систему предотвращения атак, поведенческий антивирус, сигнатурный антивирус, шлюз VPN, фильтрацию доступа к веб-сайтам и их контента, анти-спам (обеспечивает проверку фишинговых ссылок в e-mail и проверку вложенных файлов). Все эти системы работают в режиме реального времени и не требуют вмешательства администратора безопасности.

Symantec Web Gateway - инновационный комплекс для защиты веб-шлюзов от угроз Web 2.0 (потенциально опасные URL, шпионские программы, ботнеты, вирусы и другие виды вредоносного ПО), который предоставляет возможность контроля над использованием сети и приложений. Symantec Web Gateway поддерживается **Symantec Global Intelligence Network** и строится на масштабируемой платформе, обеспечивая быстрое и полное сканирование на наличие вредоносного ПО и неадекватного веб-содержимого, за счет чего поддерживается стабильная и бесперебойная работа важных ресурсов сети и минимизируются риски снижения производительности труда сотрудников, которые при атаках страдают в первую очередь.

Тем, кому требуется защитить корпоративную сеть от шпионских и вредоносных программ, предотвратить доступ сотрудников к представляющим угрозу веб-узлам или **управлять распространением конфиденциальной информации** через веб-шлюзы, компания LETA предлагает доступное решение **McAfee Web Gateway** (ранее Webwasher). В одном устройстве McAfee Web Gateway объединены многочисленные средства защиты, для использования которых в противном случае потребовалось бы несколько отдельных продуктов, таких как веб-фильтр, антивирусное и антишпионское программное обеспечение, SSL-сканер и фильтры управления содержимым. Упреждающая защита от незнакомых вредоносных программ объединена с комплексным антивирусным модулем на основе сигнатур для защиты от известных вредоносных программ.

Построение корпоративной системы шифрования данных

Используемые технические решения:

- McAfee Endpoint Encryption
- Symantec Endpoint Encryption
- Aladdin Secret Disk
- ИнфоТеКс ViPNet SafeDisk

Шифрование данных (криптографическая защита данных) – важный элемент системы информационной безопасности, обеспечивающий надежную сохранность конфиденциальной информации. Шифрование данных позволяет свести к минимуму угрозы утечки конфиденциальной информации через третьих лиц даже в случае получения ими доступа к зашифрованным файлам (утраченный, забытый и т.п. носитель).

Защита персональных данных от утечки стала обязательной в связи с принятием в России Федерального закона № 152-ФЗ «О персональных данных». Шифрование данных включено рядом мировых стандартов по обеспечению информационной безопасности (например, PCI DSS) в число обязательных условий соответствия установленным нормам.

В России необходимость защиты конфиденциальной информации и персональных данных от утечек средствами систем шифрования данных подтверждается также растущей популярностью электронного документооборота, электронных архивов, центров обработки данных. Важность электронных документов, циркулирующих внутри организаций и между ними, диктует все более высокие требования к обеспечению их защиты.

Построение корпоративной системы шифрования данных предполагает внедрение линейки программных продуктов отечественных и зарубежных разработчиков. Они отличаются алгоритмами шифрования – преимущественно ГОСТ и AES, DES (и другие) соответственно. Выбор конкретного решения определяется задачами Заказчика и принятыми нормами и правилами – как корпоративными, так и прописанными в законодательстве.

Корпоративная система шифрования данных от LETA IT-company совмещает две минимально необходимые составляющие – возможности криптопровайдера (криптоядра с определенным алгоритмом шифрования) и системы защиты, непосредственно осуществляющей шифрование с применением внешнего криптопровайдера. Криптографические средства защиты информации позволяют гибко реализовывать корпоративную систему шифрования данных, обеспечивая шифрование файлов, каталогов, виртуальных и жестких дисков, флеш-накопителей, серверов, а также формирование и проверку электронно-цифровой подписи (ЭЦП), служащей для организации юридически значимого документооборота.

Корпоративная система шифрования данных от LETA IT-company основывается на сертифицированных решениях отечественных разработчиков.

В качестве средства защиты в серверных решениях **LETA IT-company применяет** программно-аппаратный комплекс **Secret Disk NG**, обеспечивающий защиту данных:

- на основных разделах, логических дисках и динамических томах жестких дисков;
- на съемных дисках;
- в файл-контейнерах.

Для защиты персональных рабочих станций используется **Secret Disk 4** — система шифрования конфиденциальной информации и персональных данных.

Программное решение **ViPNet SafeDisk**, также применяемое LETA IT-company при построении корпоративной системы шифрования данных, предназначено для защиты конфиденциальных и персональных данных. Создание зашифрованного контейнера с конфиденциальной информацией реализовано собственными средствами продукта (без использования встроенных механизмов операционной системы), предназначено для организации безопасного хранения конфиденциальной информации и удобной работы с ней на персональном компьютере.

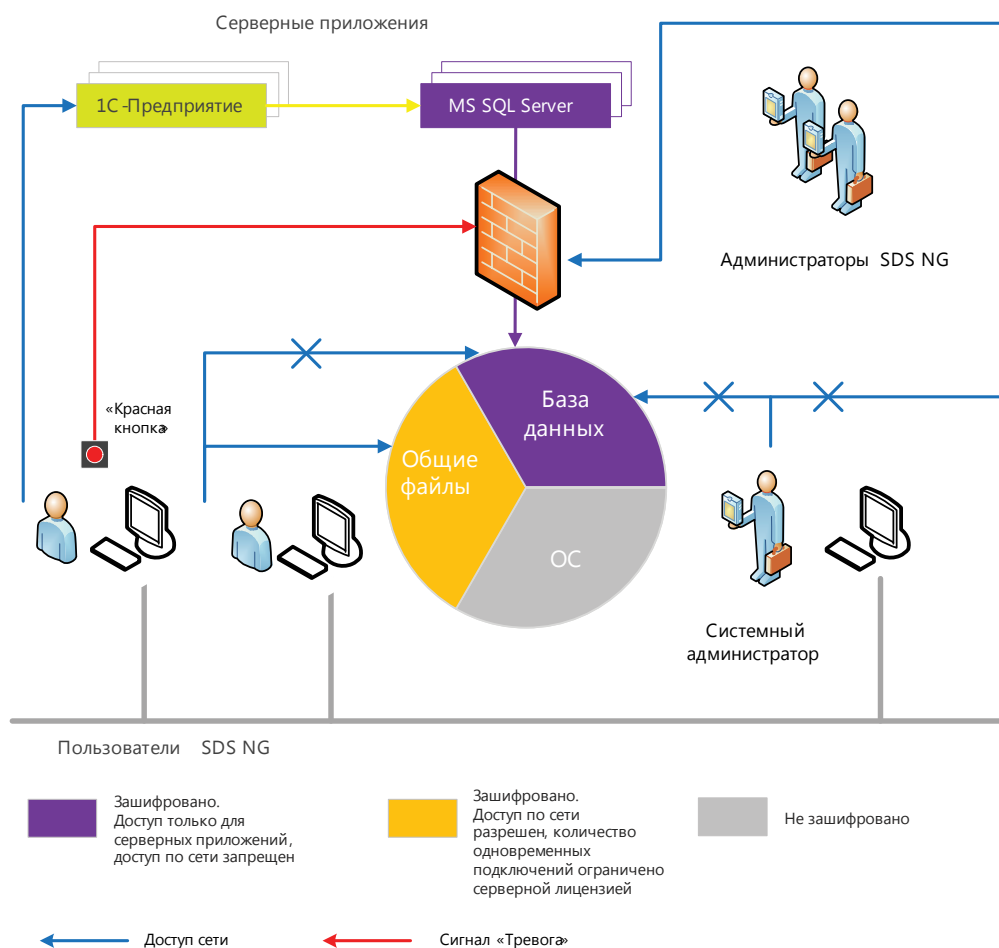


Рисунок. Принцип работы Secret Disk NG

McAfee Endpoint Encryption состоит из нескольких взаимосвязанных модулей, которые реализуют несколько уровней защиты от утечек данных. Решение обеспечивает надежную криптозащиту настольных и портативных компьютеров, общих папок, мобильных устройств, съемных носителей и переносных устройств хранения. Для защиты данных применяются ведущие отраслевые технологии шифрования, включая **AES 256** и **RC5 1024**. Поддержка однократной регистрации, аутентификация с использованием портативных устройств и возможность пользователя самостоятельно восстановить пароль при работе офлайн гарантируют максимальную безопасность данных без ущерба для удобства работы. Пакет Endpoint Encryption прозрачно интегрируется с другими продуктами безопасности McAfee, а также с существующими компонентами корпоративной инфраструктуры, что позволяет реализовать всестороннюю защиту при минимальных затратах на внедрение и сопровождение.

Symantec Endpoint Encryption 7.0 обеспечивает улучшенное шифрование для рабочих станций, портативных компьютеров и съемных устройств хранения данных. Этот продукт обеспечивает масштабируемую защиту всего предприятия и предотвращает несанкционированный доступ благодаря надежным функциям управления доступом и шифрования. В состав Symantec Endpoint Encryption входит консоль централизованного управления, обеспечивающая безопасное централизованное развертывание и управление шифрованием на конечных точках.

Построение корпоративной системы идентификации и аутентификации

Используемые технические решения:

eToken TMS (разработчик – Aladdin)

Корпоративная система идентификации и аутентификации обеспечивает аппаратную авторизацию пользователей при доступе к информационным ресурсам Компании на основе токенов – компактных устройств в виде USB-брелоков и смарт-карт, содержащих личную информацию. Токены могут применяться для хранения многосимвольных сложных паролей, персональных данных пользователей, цифровых сертификатов, ключевой информации (при использовании сервисов, основанных на ЭЦП), бесконтактных «электронных проходных», использоваться при интеграции с системами контроля и управления доступом в помещения (СКУД), системами учета рабочего времени персонала и т.д. Благодаря своей многофункциональности токены облегчают повышение уровня корпоративной информационной безопасности и уровня дисциплины сотрудников Компании.

В рамках услуги по построению корпоративной системы идентификации и аутентификации LETA IT-company применяет системы, основанные на использовании:

- защищенных носителей ключевой информации (USB-ключей и смарт-карт с защищенной памятью), позволяющих повысить безопасность ИС за счёт использования строгой двухфакторной аутентификации;
- технологии одноразовых паролей (One Time Password), позволяющей повысить безопасность ИС при удалённом доступе к корпоративным ресурсам из недоверенных сред;
- технологии единого входа (Single Sign On), позволяющей обеспечить прозрачный вход в различные приложения с безопасным хранением аутентификационных данных на защищённых носителях ключевой информации.

Корпоративная система идентификации и аутентификации от LETA IT-company обеспечивает организации-заказчику:

- интеграцию с системами контроля и управления доступом (СКУД);
- повышение уровня безопасности и строгий контроль за доступом и учетными данными;
- увеличение производительности работы сотрудников и упрощение процедуры доступа к системам и данным;
- существенное уменьшение объема административной работы.

Построенная LETA IT-company система идентификации и аутентификации также позволяет пользователям организации-заказчика:

- повысить защищенность своей информации и обеспечить к ней безопасный доступ;
- всегда иметь при себе персональные цифровые данные (сертификаты ЭЦП, ключи шифрования, коды доступа), хранящиеся в защищенной памяти;
- значительно снизить риск раскрытия используемых аккаунтов;
- проходить единую аутентификацию в приложениях;
- использовать одноразовые пароли при подключении через Интернет.

Организационные политики



Построение корпоративной инфраструктуры открытых ключей - PKI (Корпоративный Удостоверяющий центр - УЦ)

Используемые технические решения:

КриптоПро УЦ

ИнфоТеКс ViPNet Custom

Одним из методов обеспечения защиты электронного документооборота, систем шифрования данных или систем аутентификации является использование системы электронно-цифровой подписи (ЭЦП).

Для осуществления данной технологии необходим выпуск сертификатов открытых ключей - PKI (Public Key Infrastructure) для уполномоченных лиц и реализации установленных правил, создание и поддержание единого пространства доверия сертификатам ЭЦП для информационных систем и ресурсов.

Зачастую при создании корпоративных систем ЭЦП, систем шифрования данных или системы аутентификации компании сталкиваются с необходимостью развертывания собственного Удостоверяющего центра для создания инфраструктуры открытых ключей.

Рассмотрим подробнее на примере корпоративной системы ЭЦП, для чего это нужно.

На первый взгляд, система ЭЦП надежна, прозрачна и обеспечивает заявленный уровень безопасности. Это всё так, но при детальном анализе выясняется, что у нее есть своя уязвимость, при которой существует угроза атаки «man in the middle» (в переводе на русский язык – «человек посередине» или «злоумышленник посередине»), и которая может существенно повлиять на деятельность компании в целом, причем не в лучшую сторону. Как мы знаем, в системе ЭЦП два ключевых элемента: секретный и открытый ключ. Секретный ключ мы храним в защищенном виде или недоступном для злоумышленника месте, а открытый ключ должен быть доступен всем участникам системы ЭЦП, поэтому мы храним его открыто или пересылаем по открытым каналам связи всем абонентам. Такая незащищенность и вызывает угрозу атаки «man in the middle». Ведь злоумышленник, имеющий физический доступ к месту хранения открытых ключей или каналам связи, по которым передается открытый ключ, может перехватить его и, создав свою пару «секретный/открытый ключ», подменить пересылаемый открытый ключ своим. В таком случае пользователь, получивший подмененный открытый ключ, будет воспринимать данные, подписанные злоумышленником, как отправленные и подписанные реальным отправителем. Проще говоря, злоумышленник сможет отсылать документ от имени другого пользователя.

Проблема уязвимости открытых ключей, используемых в различных криптографических системах, при пересылке или хранении решается созданием инфраструктуры открытых ключей (PKI).

Как правило, в состав исполнительного комплекса PKI входят следующие основные компоненты:

- Удостоверяющий центр (Certificate Authority, Certificate Manager и т.п.) – главная компонента PKI, предназначенная для выпуска и управления сертификатами, управления базой данных инфраструктуры открытых ключей, назначения политики безопасности для всей организации;
- Регистрационный центр (Registration Authority, Registration Manager и т.п.) - компонент структуры PKI, обеспечивающий функции по аутентификации пользователей и составлению запроса на сертификацию.

В зависимости от поставщика решения в этот комплекс может входить дополнительное программное обеспечение, обеспечивающее следующие функции:

- хранение и восстановление секретных ключей пользователей;
- прием удаленно представленных запросов на получение сертификата (по электронной почте, для систем VPN или от веб-браузеров) и распределение полученных сертификатов;
- поддержку криптографических аппаратных устройств.

Внедрение корпоративной PKI позволит:

- создать максимально защищенную корпоративную систему ЭЦП;
- использовать ключевую инфраструктуру в системах шифрования данных (защита конфиденциальной информации при передаче по различным каналам связи, системы защищенного хранения данных и др.);
- повысить степень доверия клиентов и поставщиков (к предоставляемым сервисам компании, электронный документооборот и др.), подтвердив свою подлинность через доверенный УЦ;
- применять двухфакторные системы аутентификации (Token, SmartCard) вместо однофакторной (Login/Password);
- значительно снизить риск раскрытия пользовательских аккаунтов.

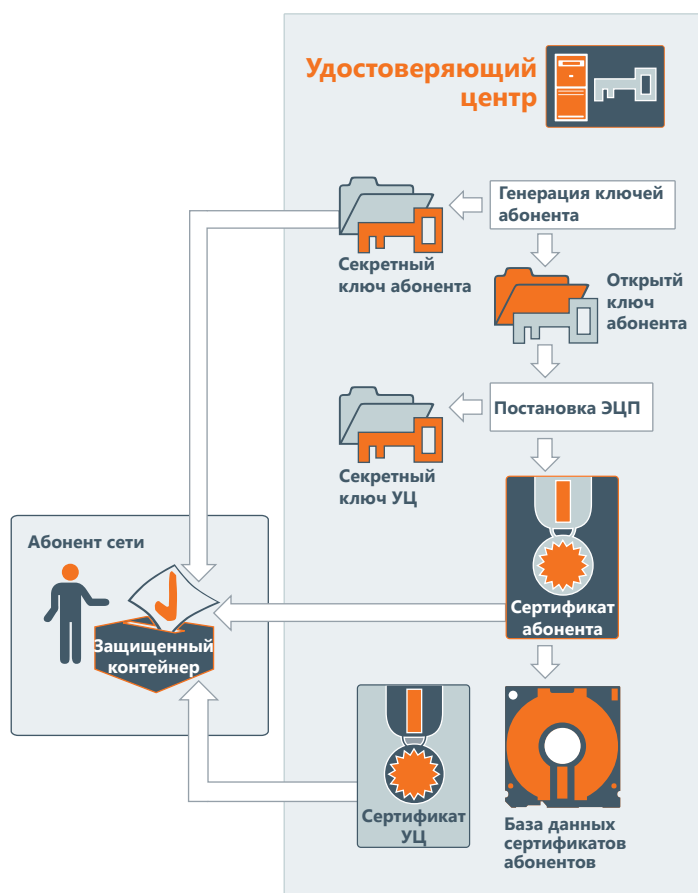


Рисунок. Схема работы Корпоративного Удостоверяющего центра

Построение системы антивирусной защиты серверов и рабочих станций

Используемые технические решения:

- Symantec
- ESET
- Trend Micro
- McAfee
- Microsoft

Внедрение комплексной корпоративной системы антивирусной защиты **снижает риски потери или утечки информации, сокращает издержки** на внедрение и эксплуатацию парка разнородных защитных систем, позволяет предотвратить и устранить последствия вирусной атаки, восстановить работоспособность ИТ-инфраструктуры.

Проникновение в сеть и заражение компьютеров сети вредоносным программным кодом являются сегодня наиболее распространенной **угрозой корпоративной безопасности**. Пути проникновения компьютерных вирусов, «червей», «троянов» и т.д. в сеть служат «обычные» в повседневной работе источники – носители информации (**CD, DVD, USB** и др.), соединения через локальную сеть Интернет, электронная почта. **Последствия проникновения** вредоносного кода в корпоративную сеть могут быть различными:

- уничтожение важной информации;
- кража конфиденциальной информации;
- несанкционированное использование сетевых ресурсов;
- несанкционированная рассылка электронных писем, в том числе спама;
- удаленное управление компьютером;
- несанкционированная атака на чужой сервер и многое другое.

Внедрение комплексной корпоративной системы антивирусной защиты обеспечивает:

- **контроль всех** возможных **каналов** проникновения вирусов: электронной почты, разрешенных для взаимодействия с Интернетом сетевых протоколов (HTTP, FTP), внешних носителей информации (дискеты, CD, DVD, flash-карты и др.), данных файловых серверов
- **защиту от** различных видов **угроз**: вирусов, сетевых и почтовых «червей», «троянских коней», нежелательных программ (spyware, adware и др.);
- **непрерывный** антивирусный **мониторинг** и периодическое антивирусное сканирование всех серверов и рабочих станций;
- **автоматическое оповещение** при «заражении», «лечение» вирусов;
- защиту **мобильных устройств** и др.

В рамках построения корпоративной системы антивирусной защиты **LETA IT-company предлагает** ряд услуг, состав которых варьируется в зависимости от потребностей компании-заказчика и может включать:

- **подготовку предложения по выбору решения антивирусной защиты (AB3);**
Возможность для Заказчика предусмотреть риски по совместимости, масштабируемости системы, выделению дополнительных аппаратных мощностей и т.д., которые могут возникнуть во время эксплуатации;
- **развертывание решения на ограниченном сегменте;**
Снижение для Заказчика возможных рисков внедрения за счет использования результатов «пилотной» эксплуатации;
- **подготовку инструкции по дальнейшему развертыванию на базе результатов развертывания на ограниченном сегменте;**
Методические рекомендации LETA IT-company по развертыванию решения на других сегментах сети на основе результатов успешного «пилотного» внедрения при реализации силами Заказчика;
- **два варианта внедрения;**
Инсталляция и конфигурирование полного решения, при которых возможны две схемы: «полная», когда развертывание на 100% объектов информационной системы выполняет LETA IT-company, и «каркасная», когда LETA IT-company проводит 10–50% объема работ по внедрению решения на стандартизированных рабочих местах и точках информационной системы с нетиповой конфигурацией, а оставшуюся часть Заказчик осуществляет самостоятельно;
- **разработку корпоративного стандарта системы AB3;**
Стандартизация требований к системе антивирусной защиты в части установки, настройки и эксплуатации ее компонент;
- **разработку инструкционных (эксплуатационных) документов системы AB3;**
Для администраторов и пользователей;
- **разработку частной политики AB3;**
Концепция принципов, подходов и требований к обеспечению антивирусной защиты информационных ресурсов Компании;
- **подготовку и проведение внутреннего семинара.**
Ознакомление всех участвующих в работе решения сотрудников Заказчика с вводимой политикой и регламентами AB3.

Построение корпоративной системы защиты каналов связи

Используемое техническое решение:

- ИнфоTeKC ViPNet Custom
- S-Terra
- StoneSoft VPN

В качестве канала передачи данных большинство предприятий сегодня активно использует публичные каналы связи: Интернет, телефонные и телеграфные коммуникации и т.п. Однако они не защищают пересылаемую конфиденциальную информацию от основных угроз при передаче по открытым каналам связи – перехвата и компрометации. Утечка информации может нанести организации серьезный материальный ущерб. Поэтому защита корпоративной информации, передаваемой по открытым публичным каналам, – актуальная потребность бизнеса подавляющего числа организаций.

Корпоративная система защиты каналов связи от LETA IT-company обеспечивает Заказчику доверенную и защищенную от потенциальных нарушителей среду для передачи конфиденциальной информации по публичным каналам связи, гарантирующую ее целостность и достоверность.

Основные преимущества от построения корпоративной системы защиты каналов связи

- **для корпоративных и частных пользователей:**
недорогое и эффективное решение по защите канала передачи корпоративной и личной информации от несанкционированных проникновений из Интернета;
- **для малого и среднего бизнеса:**
эффективные, интегрированные и защищенные коммуникации в едином решении, ранее доступные только крупным корпорациям. Корпоративная система защиты каналов связи позволяет при использовании общедоступного канала доступа в Интернет интегрировать в одно целое функциональность ряда прикладных защитных программ без опасения потери, искажения или кражи важной для бизнеса информации;
- **для крупного бизнеса:**
возможность превратить все «тяжелые» и затратные системы в сфере корпоративных сетей в более гибкие, недорогие и при этом не менее функциональные решения на базе интернет-/интранет-технологий без опасения потери конфиденциальной информации;
возможность для топ-менеджмента не зависеть от ИТ-подразделений: решения для защиты каналов связи используют отдельные центры управления безопасностью и сетью и позволяют руководству корпорации вести самостоятельный визуальный контроль за состоянием всей сети.

Корпоративная система защиты каналов связи строится на базе новейших комплексов программного и программно-аппаратного обеспечения российских и зарубежных производителей.

ViPNet Custom - это сертификат ФСТЭК России (Гостехкомиссии России) на соответствие необходимым классам защищенности и уровням доверия. Решение включает более 10 различных компонент и модулей, позволяющих реализовать множество сценариев защиты информации в современных мультисервисных сетях связи. Имеет возможность объединять в единую защищенную виртуальную сеть произвольное число локальных сетей и рабочих станций. Позволяет комбинировать гибкий набор компонент и их функций для любых потребностей небольших структур (объединение нескольких компьютеров через открытые каналы связи) и крупных коммерческих и государственных организаций (большие территориально распределенные сети). Имеет дополнительные возможности защищенного обмена информацией (встроенные службы мгновенного обмена сообщениями – чат и конференция, файлами, собственная защищенная почтовая служба с элементами автоматизации обмена письмами и поддержкой

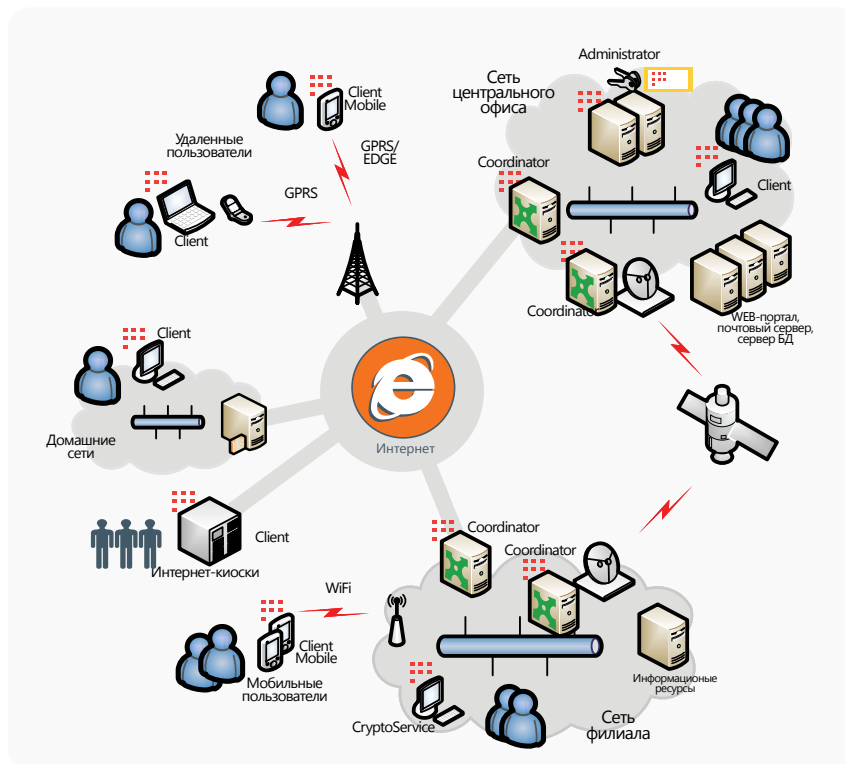


Рисунок. Примеры использования ViPNet для защиты сетей различных масштабов

минимизировать затраты на систему безопасности в целом (контроль сетевой активности приложений, строгий контроль доступа к Интернету, механизмы аварийной перезагрузки и защиты от вторжений на этапе загрузки операционной системы). Существует возможность установки и настройки на уже существующем компьютерном парке Заказчика (без специализированного оборудования).

Для построения корпоративной системы защиты каналов связи также возможно использование решения компании **C-Терра СуЭсПи** - сочетание некриптографических средств защиты информации от компании Cisco Systems и сертифицированных продуктов сетевой защиты **CSP VPN**. Продукты линии CSP VPN разработаны для того, чтобы работать в той же инфраструктуре безопасности, что и продукты **Cisco Systems**. Использование единой инфраструктуры позволяет взаимоувязать систему безопасности в рамках сети и согласовать функции средств защиты информации, входящих в её состав.

В основе межсетевого экрана с интегрированными функциями построения VPN **StoneGate Firewall/VPN** лежат уникальные архитектурные решения, позволяющие обеспечить непревзойденный уровень защиты информационных систем. В StoneGate FW/VPN используется собственная интегрированная защищенная ОС, что исключает необходимость выполнения каких-либо специализированных операций по настройке (все необходимые инсталляции выполняются в «один проход»), а также позволяет наращивать функциональность StoneGate лишь за счет добавления новых компонентов без изменения работающей инфраструктуры и без остановки в работе. В StoneGate FW/VPN применены самые современные технологии анализа трафика и обеспечения отказоустойчивости.

Решение **StoneGate FW/VPN** имеет большое количество сертификатов признанных международных организаций по информационной безопасности, таких как **VPN Consortium, ICSA Labs, Common Criteria** (с уровнем доверия EAL4+). StoneGate FW/VPN проходит сертификацию во ФСТЭК России по 2-ому классу защищенности для межсетевых экранов. В настоящее время проводится сертификация на контроль НДВ по 4-му уровню как распределенный МЭ по схеме сертификации производства, а также для применения в ИСПДн до класса К1 включительно.

При построении защищенных VPN StoneGate Firewall позволяет использовать не только зарубежные криптоалгоритмы, но и модуль шифрования с сертифицированным **ФСБ России** российским криптопровайдером **Крупто Про**.

Построение системы обнаружения и предотвращения вторжений

Используемые технические решения:

- Stonesoft StoneGate IPS
- IBM Proventia Network IPS
- McAfee Network Security Platform
- ESET NOD32 Firewall

Корпоративная система предотвращения атак предоставляет информацию обо всех потоках данных, поступающих в корпоративную сеть из удаленных источников, блокирует либо оповещает о выявленных потенциальных опасностях и позволяет за счет проактивного подхода более эффективно применять средства защиты информации против запланированных враждебных воздействий. Корпоративная система предотвращения атак является составной частью стратегии безопасности предприятия и обеспечивает организациям наиболее масштабируемый, гибкий и полный метод безопасной, надежной, экономичной и эффективной конкуренции в мире электронного бизнеса.

Корпоративная система предотвращения атак от LETA IT-company может быть ориентирована на предприятия разных масштабов: от уровня малого и среднего бизнеса до уровня крупных корпораций.

Системы предотвращения атак:

- используют различные методы обнаружения вторжений (сигнатурный анализ, технология декодирования протоколов, анализ аномалий протоколов, обнаружения любых видов сканирования сетей, адаптивное применение сигнатур);
- проводят анализ и корреляцию событий безопасности на предмет наличия шаблонов, отражающих злоупотребления или необычные особенности «поведения»;
- позволяют автоматически реагировать на обнаруженную подозрительную активность;
- генерируют отчет с результатами, полученными в процессе обнаружения.

Стратегия действий злоумышленника часто включает проведение атак или вывод из строя устройств защиты, обеспечивающих безопасность конкретной цели. Корпоративная система предотвращения атак контролирует работу межсетевых экранов, шифрующих маршрутизаторов, основных серверов и файлов, являющихся важными элементами других механизмов защиты, и тем самым обеспечивает для обслуживаемой корпоративной системы дополнительные уровни защищенности. Система распознает первые признаки атаки и реагирует на них, минимизируя возможные последствия полной неготовности к «нападению». В случае сбоев или отказа других защитных устройств (из-за ошибок конфигурации, пользователей, атаки и т.д.), не всегда заметного сразу, система обнаружения атак вовремя распознает проблему и выдает службе информационной безопасности оповещение, позволяющее оперативно принять меры против заранее выявленных угроз.

Пропущенная атака может обойтись бизнесу крайне дорого. Не обнаруженные вовремя DoS-атаки уже неоднократно выводили из строя платежные системы банков, позволяя злоумышленникам пользоваться простотой компонентов систем в корыстных целях. Довольно часто фиксируются случаи банкротства компаний в результате грамотно спланированных атак на ресурсы корпоративной сети.

Stonesoft StoneGate IPS - это модульная высокоэффективная система защиты критически важных для бизнеса сервисов и данных как в физической, так и в виртуальной среде. StoneGate IPS реализует механизмы проактивной защиты, обнаруживая, идентифицируя и предотвращая распространение вредоносного трафика. Технология IPS Transparent Access Control позволяет с легкостью сегментировать существующую сетевую инфраструктуру. Подобная сегментация позволяет разделить вашу сеть на ряд зон с различными требованиями по безопасности, выделив и защитив наиболее ценные активы.



Рисунок. Принцип работы StoneGate IPS

Система предотвращения атак **IBM Proventia Network IPS** предназначена для блокирования сетевых атак и аудита работы сети. Благодаря запатентованной технологии анализа протоколов решение **IBM Internet Security Systems** обеспечивает превентивную защиту – своевременную защиту корпоративной сети от широкого спектра угроз. Превентивность защиты основана на круглосуточном отслеживании угроз в центре обеспечения безопасности GTOC и собственных исследованиях и поисках уязвимостей аналитиками и разработчиками группы X-Force.

По статистике, не менее 75% всех компьютерных преступлений происходит внутри корпоративной сети – по вине сотрудников предприятия. Традиционные средства защиты (например, межсетевые экраны) не позволяют защитить корпоративную сеть от умысла злоумышленника, имеющего в нее доступ в рамках рабочих полномочий. Для построения эффективной системы защиты информации нужны дополнительные средства предотвращения атак.

Платформа сетевой безопасности **McAfee® Network Security Platform** (ранее McAfee IntruShield) обеспечивает интегрированную, автоматическую и готовую к действию защиту, основанную на знании отрасли. Network Security Platform сочетает инфраструктуру сетевой и системной безопасности для активной защиты всего предприятия. Она в несколько раз точнее и эффективнее, чем традиционные продукты для конечных точек. Управление риском и соответствие требованиям требует меньших усилий. Интеллектуальная безопасность и надежные платформы сетевого класса обеспечивают полную уверенность в безопасности.

Для защиты инфраструктуры сети от атак очень удобно применение многофункционального программно-аппаратного межсетевого экрана класса «все в одном», примером которого является решение **ESET NOD32 Firewall**. Продукт включает в себя системы обнаружения и предупреждения сетевых атак, систему защиты от вирусов ESET NOD32 и защиты от спама. Правила, интегрированные в систему выявления сетевых атак, учитывают большинство атак, которым подвержены сетевые службы.

Построение корпоративной системы межсетевого экранирования

Используемые технические решения:

- Stonesoft StoneGate Firewall/VPN
- ИнфоТеКC ViPNet Custom
- Microsoft Threat Management Gateway
- Check Point UTM-1

В настоящее время обычная **корпоративная локально-вычислительная сеть** представляет собой, как правило, **распределенную сеть передачи данных**, включающую в себя множество сетевых сегментов разного уровня доступа, как обмен данными между территориально удаленными офисами, так и доступ в сеть Интернет, с привлечением различных видов сервиса и служб.

Становление и глобальное развитие сети Интернет и сетевой инфраструктуры отечественных компаний привело к **увеличению угроз вредоносных атак** со стороны потенциальных злоумышленников. Проникновение злоумышленника к ресурсам и базам данных Компании несет за собой **хищение и искажение конфиденциальной информации Компании**, что приводит к громадному ущербу организации.

Услуга «**Построение корпоративной системы межсетевого экранирования**», предоставляемая с использованием межсетевых экранов (firewall), направлена на **обеспечение безопасного подключения корпоративной сети к сетям общего пользования** на базе сетевых протоколов, построение надежной защиты периметра организации, обеспечение контроля за информационными потоками между сегментами корпоративной сети, а также **разграничение доступа к внутренним** (публикуемым) **ресурсам** корпоративной сети извне.

Также услуга предполагает **создание частной политики информационной безопасности** (политика межсетевого экранирования), что позволит четко сформулировать принципы защиты и подход Компании к построению системы межсетевого экранирования.

В рамках оказания услуги специалисты LETA IT-company выполняют следующие работы:

- обследование существующей сетевой инфраструктуры Заказчика;
- разработка и согласование Технического задания;
- разработка и согласование программы и методики испытаний;
- разработка частной политики информационной безопасности (политики межсетевого экранирования);
- установка, конфигурирование и настройка компонентов системы;
- интеграция системы в информационную инфраструктуру Заказчика;
- разработка регламентов и эксплуатационной документации;
- обучение персонала.

Полноценная система межсетевого экранирования дает Заказчику следующие преимущества:

- повышение уровня защищенности корпоративной сети;
- снижение финансовых и бизнес-рисков Компании от несанкционированного доступа к ее сети и информационным ресурсам;
- четкая регламентация информационных потоков в/из локальной вычислительной сети организации;
- формализованный процесс обращения к ресурсам Компании за счет внедрения частной политики информационной безопасности;
- снижение количества инцидентов, связанных с хакерскими атаками, умышленными и неумышленными действиями пользователей, проникновения вредоносного кода;
- выявление попыток нарушения принятой политики информационной безопасности за счет использования средств мониторинга и протоколирования событий.

Большую роль в защите конфиденциальной информации и персональных данных играет наличие установленных межсетевых экранов, имеющих **сертификаты ФСТЭК России** и соответствующих требованиям руководящего **документа Гостехкомиссии России** «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

LETA IT-company готова предложить Заказчикам решение задач по **разграничению доступа между различными сетями любого уровня сложности** и **рекомендации по построению защищенного периметра сети** как с учетом необходимых требований и стандартов российского законодательства, так и установленных внутри предприятия.

StoneGate Firewall/VPN – это линейка программных и программно-аппаратных межсетевых экранов с возможностью построения отказоустойчивых VPN, в том числе с использованием российских криптографических алгоритмов. Производительность межсетевых экранов – от 100 Мб/с до 25 Гб/с, что позволяет удовлетворить потребности предприятий и организаций любого масштаба.

StoneGate Firewall/VPN имеет сертификаты ГОСТ Р, Минсвязи, сертификат ФСБ на СКЗИ (за счет использования сертифицированных криптоалгоритмов), сертификат ФСТЭК на соответствие ТУ, по 2-му классу для МЭ и 4-му уровню контроля отсутствия НДВ, а также может использоваться для защиты информации в информационных системах персональных данных до класса К1 и автоматизированных системах класса 1В включительно.

Особенности продукта:

- централизованная система управления FW, IPS и SSL;
- поддержка российских и зарубежных алгоритмов шифрования;
- функции кластеризации, высокой доступности и балансировки нагрузки по каналам связи, пулу серверов, в VPN-соединениях;
- защита от вирусов, spyware.

Построение системы удаленного защищенного доступа

Используемые технические решения:

- Check Point Connectra
- Stonesoft StoneGate SSL VPN
- Aladdin eToken TMS

Система защищенного удаленного доступа позволяет организовать работу с внутренними информационными ресурсами Компании сотрудникам и партнерам, работающим вне офиса – с домашнего компьютера, через Wi-Fi-доступ в аэропортах, кафе, торговых центрах, интернет-кафе, через сеть партнера по бизнесу и т.д. Система решает для Заказчика три основные задачи, обеспечивая связь, управление и безопасность.

Система защищенного удаленного доступа от LETA IT-company предоставляет:

- безопасный доступ к корпоративной почте, внутренним корпоративным веб-порталам и сервисам, FTP-серверам и папкам общего доступа в любое время из любого места;
- защищенное удаленное подключение к внутренним серверам Компании для проведения административных задач, когда сбои в работе сети выявляются при отсутствии персонала на рабочем месте (ночью, в праздничные дни, во время отпусков и т.п.);
- защищенный доступ к сетевым приложениям – управления взаимоотношениями с клиентами (CRM), управления цепочками поставок (SCM), планирования и управления ресурсами предприятия (ERP) или другим специализированным корпоративным приложениям, что оптимизирует ключевые бизнес-процессы и расширяет возможности пользователей.

Удаленные рабочие станции могут содержать вредоносные, шпионские программы и не иметь средств обеспечения безопасности (антивирусной защиты, персонального межсетевого экрана), тем самым подвергая корпоративную информационную систему Компании дополнительным угрозам безопасности и рискам атак. Поэтому защищенный удаленный доступ к ресурсам организации должен осуществляться с компьютера, управляемого Компанией. Для защиты от несанкционированного доступа к информации также необходима аутентификация пользователей с использованием электронных ключей.

Эффективным решением для обеспечения защищенного удаленного доступа к корпоративным ресурсам организации из любой точки с помощью стандартных веб-браузеров является организация виртуальной частной сети SSL VPN.

Check Point Connectra – шлюз, обеспечивающий защиту корпоративной сети при использовании ее ресурсов удаленными пользователями. Connectra остается одним из наиболее востребованных продуктов, гарантирующих безопасность удаленных точек подключения и сети в целом. В состав пакета Connectra входят лучшие в отрасли инструменты организации виртуальных частных сетей SSL VPN, включая встроенные технологии Web Intelligence и Application Intelligence, инструменты выявления шпионских программ, функцию безопасного просмотра ресурсов Интернета, встроенный защищенный браузер с поддержкой шифрования данных на удаленной системе, и т.д.

Надежную аутентификацию пользователей при удаленном доступе к сетевым ресурсам и существенное снижение рисков утечки информации обеспечит интеграция Check Point Connectra с системой управления жизненным циклом USB-ключей и смарт-карт Aladdin eToken TMS (Token Management System).

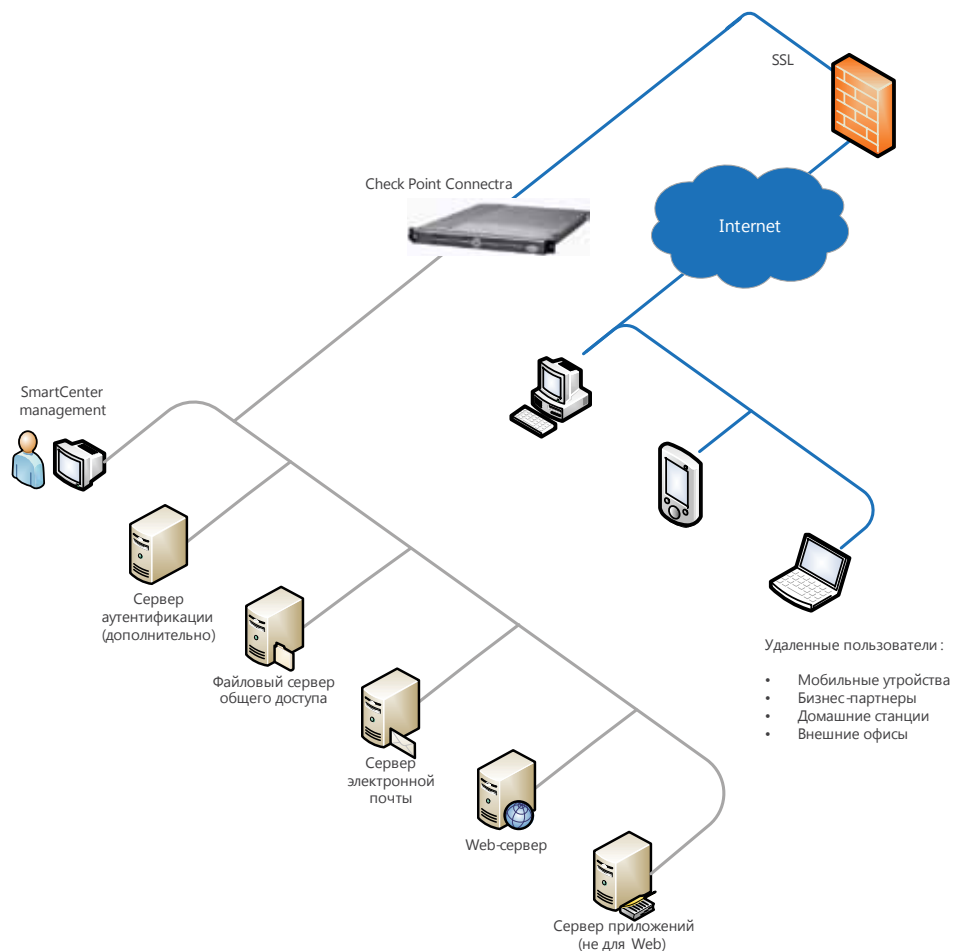


Рисунок. Схема построения системы защищенного удаленного доступа

Решение Stonesoft StoneGate SSL VPN является идеальным выбором для организаций, которым необходимо обеспечить безопасный, но в то же время достаточно гибкий удалённый доступ к своим ресурсам для партнёров, клиентов и персонала. Доступ к различным приложениям может быть разграничен на основе данных учётной записи пользователя, метода аутентификации, адреса клиента и уровня безопасности клиентского устройства. Решение обеспечивает полную защиту корпоративных ресурсов, одновременно с этим предоставляя к ним доступ авторизованных пользователей из любой точки мира.

Решения Stonesoft StoneGate SSL VPN и Check Point Connectra также позволяют построить защищенный удаленный доступ на сертифицированных российских криптоалгоритмах.

Построение системы резервного копирования и восстановления данных

Используемые технические решения:

- Symantec Backup Exec
- Symantec Backup Exec System Recovery
- Symantec Net Backup

Самое ценное в любой информационной системе, во имя чего она, собственно, и существует, — это хранящиеся в ней данные. Но как бы ни были надежны аппаратные средства, как бы хорошо ни было протестировано программное обеспечение, всегда существует **вероятность потери информации**. Информация в вычислительных сетях может быть **утрачена по следующим причинам** (в процентном соотношении):

- аварии аппаратуры и программного обеспечения — 12%;
- ошибки персонала — 75%;
- вирусы — 10%;
- прочие причины (например, злой умысел) — 3%.

В ряде случаев можно предпринять меры, снижающие вероятность потери данных, например, воспользоваться передовыми техническими средствами, позволяющими достаточно надежно защитить информационную систему от аварий аппаратуры. Но даже это не исключает риска потери данных. Кроме того, от ошибок персонала защититься вообще невозможно, ибо они обусловлены самой человеческой природой. Важной частью мер, направленных на обеспечение надежного функционирования информационных систем, является **разработка технологии наиболее быстрого восстановления данных в случае их потери**, что позволит свести урон от простоя к минимуму. Решением этой задачи служит **создание развитой системы резервного копирования и восстановления данных**.

Система резервного копирования представляет собой программно-аппаратный комплекс, предназначенный для создания **дополнительных копий критически важной информации**. Система резервного копирования является одним из необходимых методов обеспечения непрерывности бизнеса. По данным Gartner, среди компаний, пострадавших от катастроф и переживших крупную необратимую потерю корпоративных данных, **43% не смогли продолжить свою деятельность**.

В отличие от систем архивирования данных, резервные копии не предназначены для долгого хранения и по мере необходимости удаляются. При этом **скорость** восстановления информации с них **значительно выше**, так как в качестве носителей могут использоваться достаточно емкие и недорогие хранилища.

LETA IT-компану пропалагае разрабтку и внедрение современных решений для резервного копирования, восстановления, обеспечения высокой доступности критически важных данных и приложений, управления ресурсами хранения, а также управления хранением файлов, электронной почты и баз данных.

Система резервного копирования и восстановления данных от LETA IT-company обеспечивает Заказчику сохранность и целостность корпоративной информации, постоянную доступность данных для пользователей и бизнес-приложений, а также восстановление работы с приложениями и данными без остановки деятельности организации.

Symantec Backup Exec - это комплексное решение, которое сочетает в себе функции защиты, восстановления, архивирования и дедупликации данных, что позволяет значительно упростить процедуру резервного копирования и восстановления самого важного ресурса организации — информации. **Symantec Backup Exec** предлагает защиту и гарантирует восстановление данных и систем вне зависимости от того, расположены ли данные на файловом сервере Windows/Linux, настольном компьютере, на виртуальном сервере либо важном сервере приложений, таком как Exchange, SQL, SharePoint, Oracle, DB2.

Продукт Symantec Backup Exec разработан с учетом растущих потребностей современных организаций и обеспечивает всестороннюю защиту данных на диске или ленте, а также **восстановление данных в средах MS Windows/Linux/VMware/Hyper-V**. Решение Backup Exec, ориентированное на работу с **дисками и накопителями на магнитной ленте** и обеспечивающее непрерывную защиту данных, избавляет от необходимости выделять специальное время для резервного копирования, ускоряет восстановление данных и позволяет конечным пользователям восстанавливать собственные файлы без вмешательства IT-специалистов. Продукт Symantec Backup Exec предлагает патентованную **технологии частичного восстановления** (GRT), которая позволяет восстанавливать данные, в том числе такую важную информацию, как отдельные электронные сообщения, папки и документы, **за считанные секунды** из одной резервной копии.

В последней версии Backup Exec, вышедшей в начале 2010 года, реализованы функции, ранее доступные только в «тяжелых» решениях, таких как NetBackup и Vault. Теперь используя в Компании продукт Backup Exec, можно использовать решение по архивированию данных, реализовав подход **ILM** (Information Lifecycle Management). Для сокращения требуемого дискового пространства для хранения резервных копий появилась возможность использовать **технологии дедупликации**, когда вместо одинаковых блоков данных хранится один из них, а в остальных случаях имеются ссылки на него.

С ростом потребностей конечных Заказчиков компания Symantec в своем продукте Backup Exec добавляет **поддержку новых платформ**, новый функционал, делающий этот продукт стандартом резервного копирования на рынке. **Недаром Microsoft для своего резервного копирования использует именно это решение.**

Symantec Backup Exec System Recovery — это комплексное, ориентированное на работу с дисками решение для восстановления систем серверов, рабочих станций и портативных компьютеров Microsoft Windows, позволяющее восстанавливать системы после аварий за считанные минуты, в том числе на других аппаратных платформах, виртуальных средах и удаленных, автономных расположениях, не тратя на это многие дни и часы. Продукт Backup Exec System Recovery является «золотым стандартом» восстановления систем Windows для сред Windows небольших компаний.

Построение системы архивирования корпоративной почты

Используемые технические решения:

- Symantec Enterprise Vault

Современная тенденция роста объемов неструктурированных данных и зависимость от электронной почты как от средства связи и обмена документами привели к ужесточению требований организаций к защите и управлению данными. Многие компании теперь рассматривают электронную почту как инструмент для решения критически важных задач.

Итак, как организации защищают передаваемые по электронной почте данные, если предполагается, что электронная почта должна быть доступна 24 часа в сутки, семь дней в неделю? И что если для решения какого-либо юридического вопроса от отдела ИТ потребуется найти файлы и электронные сообщения, относящиеся к прибылям за прошлый квартал? Имея совсем немного времени для резервного копирования, системные администраторы должны соответствовать строжайшим корпоративным требованиям. Кроме того, несмотря на экспоненциальный рост объемов информации и растущие требования пользователей к восстановлению данных, выделяемые на ИТ бюджеты остаются небольшими.

Система архивирования корпоративной почты от LETA IT-company предоставляет Заказчику интеллектуальную платформу архивирования, которая хранит, управляет и позволяет находить корпоративные данные в системах электронной почты, средах файловых серверов, на платформах мгновенного обмена сообщениями (IM), а также в системах обеспечения сотрудничества и управления содержанием. Кроме того, система архивирования корпоративной почты поможет компаниям, занятым в области финансовых операций, здравоохранения и в других областях, подлежащих серьезному контролю, поддерживать постоянный систематичный мониторинг всех корпоративных данных на предмет соответствия требованиям законодательства и стандартов.

Основные выгоды от построения системы архивирования корпоративной почты:

- **архивирование в соответствии с правовыми и нормативными требованиями;**

Сокращение расходов, связанных с поиском, отбором и предоставлением в юридические и судебные органы электронных документов по запросам; обеспечение соответствия установленным нормам хранения и контроля электронных документов; помощь в расследовании инцидентов ИБ;

- **управление жизненным циклом информации;**

Текущее хранение электронных записей данных и его прекращение по истечении установленного срока, основанное на заданных бизнес-политиках; распределение по категориям и назначение признаков; индексирование и поиск; интеграция с другими системами управления информацией;

- **управление ресурсами электронной почты;**

Оптимизация производительности службы электронной почты; сокращение времени резервного копирования и миграции данных на другие аппаратные платформы хранения; необязательность применения почтовых квот;

- **оптимизация хранения данных.**

Консолидация файл-серверов; централизованное управление PST-файлами (архивами электронной почты); функция сжатия данных и технология дедупликации (хранение не более одного экземпляра копии данных); реализация многоуровневой среды хранения.

Основной функцией Enterprise Vault является перенос данных из основного хранилища приложения во вспомогательное (как правило, менее дорогое) на основе политик. Enterprise Vault может использовать различные типы устройств хранения, но управление информацией осуществляется вне зависимости от них в соответствии с заданными политиками. Обычная политика для Exchange состоит в архивировании всех материалов старше 30 дней и замене их ярлыками или в архивировании почтовых ящиков пользователей, когда они исчерпывают 75% выделенной квоты, также с заменой материалов ярлыками.

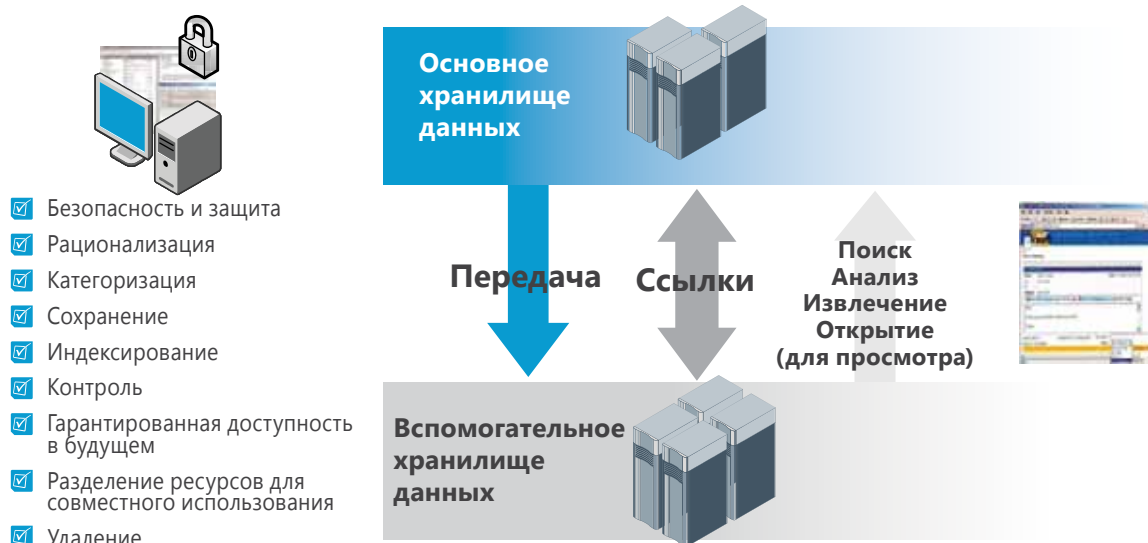


Рисунок. Принцип работы Symantec Enterprise Vault

После того, как материал перенесен в архив, нам необходимо обеспечить прозрачный доступ конечного пользователя к этому материалу. Архивирование не должно оказывать влияния на конечного пользователя. Если он оставил элемент в папке «Входящие», он должен видеть его как обычный элемент папки «Входящие», а при нажатии этот элемент должен открыться, как обычно. Такая прозрачная среда создается путем замены элементов «ссылками» или «ярлыками», она является ключевым моментом в снижении общей стоимости владения Enterprise Vault.

Услуги по защите информационных ресурсов, собственником которых является государство (государственная тайна, конфиденциальная информация)

В отношении информации ограниченного доступа, собственником которой является государство (конфиденциальная информация), установлены особые условия обработки. Они определены Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» и рядом руководящих документов регулирующих органов ФСБ России и ФСТЭК (Гостехкомиссии) России – в частности, нормативно-методическим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) Гостехкомиссии России от 30 августа 2002 г. № 282.

Компания LETA в рамках защиты конфиденциальной информации предлагает:

- аттестацию автоматизированных систем, обрабатывающих конфиденциальную информацию;
- аттестацию помещений, в которых обсуждается конфиденциальная информация;
- периодический контроль за состоянием и эксплуатацией ранее аттестованного объекта информатизации.

Эти услуги подтверждают, что объекты информатизации, обрабатывающие конфиденциальную информацию, соответствуют требованиям государственных стандартов, руководящих и нормативно-методических документов по безопасности информации, утвержденных ФСТЭК (Гостехкомиссией) России.

Внедрение данных услуг дает Заказчику:

- решение одной из необходимых задач по подготовке организации к получению лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации;
- защиту конфиденциальных переговоров/обсуждений, проходящих в аттестуемом помещении;
- повышение доверия к Компании со стороны государственных организаций, ведомств;
- повышение защиты информационных ресурсов, доверенных Компании государственными организациями/ведомствами;
- подтверждение неизменности принятых мер по защите обрабатываемой конфиденциальной информации.

Услуги по аттестации шире, чем работы, определенные в руководящем документе СТР-К ФСТЭК (Гостехкомиссии) России.

В рамках услуги «Аттестация автоматизированных систем, обрабатывающих конфиденциальную информацию» выполняются следующие работы:

- проведение объектовых исследований объекта информатизации;
- установка технических средств защиты информации от утечки по техническим каналам (средства защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок, средства защиты информации от утечки по цепям электропитания и заземления);
- проведение контроля защищенности конфиденциальной информации от утечки по техническим каналам;
- проведение контроля защищенности конфиденциальной информации от несанкционированного доступа;
- разработка материалов аттестационных испытаний.

Подтверждением успешного прохождения аттестации является Аттестат соответствия объекта информатизации требованиям по безопасности информации на срок, не превышающий 3 года.

В рамках услуги «Аттестация помещений, в которых обсуждается конфиденциальная информация» выполняются следующие работы:

- установка средств защиты информации от утечки по техническим каналам (средства защиты информации от утечки по акустическому каналу, средства защиты информации от утечки по виброакустическому каналу, средства защиты информации от утечки за счет акустоэлектрических преобразований);
- проведение контроля защищенности конфиденциальной информации от утечки по техническим каналам;
- разработка материалов аттестационных испытаний.

Подтверждением успешного прохождения аттестации является Аттестат соответствия объекта информатизации требованиям по безопасности информации, выданный на срок, не превышающий 3 года.

В рамках услуги «Периодический контроль за состоянием и эксплуатацией ранее аттестованного объекта информатизации» выполняются следующие работы:

- контроль за соблюдением требований нормативно-методических документов по защите конфиденциальной информации;
- контроль работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- контроль знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации;
- контроль неизменности состава и условий размещения технических средств обработки конфиденциальной информации;
- контроль неизменности технологического процесса обработки и перечня конфиденциальной информации.

Данные услуги осуществляются совместно с компанией «ЛОТ» – ассоциированным партнером LETA по оказанию услуг в сфере информационной безопасности. Формат консорциума позволяет реализовывать для Заказчиков специализированные проекты повышенной секретности и сложности, требующие наличия ряда уникальных лицензий и компетенций.

Стратегические партнеры LETA IT-company



Компания «ЛОТ» – ассоциированный партнер LETA по оказанию услуг в сфере информационной безопасности. Формат консорциума, в котором на постоянной основе сотрудничают LETA и «ЛОТ», позволяет реализовывать для Заказчиков специализированные проекты повышенной секретности и сложности, требующие наличия ряда уникальных лицензий и компетенций.



В рамках консорциума с компанией Digital Security, обладающей статусом QSA (Qualified Security Assessor), LETA IT-company оказывает заказчикам полный комплекс услуг по выполнению требований стандарта PCI DSS.



Ассоциированный партнер LETA по консалтингу в области управления бизнес-процессами.



Ассоциированный партнер LETA по процессному консалтингу в области ITIL | ITSM.

ЛОТ

Сотрудничество с «ЛОТ» позволяет LETA обеспечить Заказчику независимую и объективную оценку уровня информационной безопасности предприятия, его информационных рисков, оценку и снижение потенциального экономического ущерба, обоснование и обеспечение возврата инвестиций в систему защиты, оптимизацию планов защиты предприятия, повышение уровня его безопасности на 20–25%, повышение устойчивости и рентабельности бизнеса на 10–15%.

Компания «ЛОТ» обладает правами на проведение работ, связанных с:

- государственной тайной (обеспечение и создание средств защиты, оказание услуг);
- шифровальными средствами (распространение, техническое обслуживание, монтаж, наладка, установка, применение при проектировании и производстве информационных систем и комплексов телекоммуникаций);
- средствами защиты информации (сертификация, испытания);
- пожарными сигнализациями и системами видеонаблюдения (проектирование, монтаж, установка, сервисное обслуживание);
- обследованием категорированных помещений;
- аттестацией по требованиям безопасности информации.

Компания «ЛОТ» располагает широким перечнем узкоспециализированных лицензий:

- на осуществление работ с использованием сведений, составляющих государственную тайну;
- на право осуществлять проведение работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну;
- на право осуществлять проведение работ, связанных с осуществлением мероприятий и (или) оказанием услуг в области защиты государственной тайны;
- на право осуществлять проектирование средств защиты информации;
- на право осуществлять производство средств защиты информации;
- на право осуществлять деятельность по техническому обслуживанию шифровальных средств;
- на право осуществлять деятельность по распространению шифровальных средств;
- на деятельность в области создания средств защиты информации;
- на право проведения работ (лицензия ФСБ РФ):
 - по специальным исследованиям на ПЭМИН технических средств обработки информации;
 - по выявлению электронных устройств, предназначенных для негласного получения информации в помещениях;
 - по выявлению электронных устройств, предназначенных для негласного получения информации в технических средствах;
- на право (лицензия Гостехкомиссии России):
 - проведения мероприятий и (или) услуг в области защиты государственной тайны;
 - проведения работ, связанных с созданием средств защиты информации;
 - проведения работ по аттестации объектов информатизации по требованиям безопасности информации РОСС RU.0001.01БИ00;
 - осуществления мероприятий и оказания услуг по технической защите конфиденциальной информации;
 - осуществления разработки и производства средств защиты конфиденциальной информации;
- на право (лицензии Госстроя России):
 - строительства зданий и сооружений I и II уровня ответственности, осуществление функций генерального подрядчика;
 - проектирования зданий и сооружений I и II уровня ответственности;
- аттестатом аккредитации испытательной лаборатории № 72 от 28.10.2003 г.

Digital Security

Консорциум LETA IT-company и Digital Security (QSA) сформирован в целях проведения аудита и реализации требований стандарта PCI DSS.

Пакет услуг LETA IT-company ориентирован на самый широкий круг предприятий, работающих с платежными картами. Среди них: банки, интернет-магазины, торговые сети, поставщики услуг, платежные шлюзы, а также любые организации, в которых обрабатываются данные о держателях карт. LETA оказывает под ключ полный набор услуг, связанных с построением системы ИБ по требованиям PCI DSS, который включает:

- предварительный аудит;
- внедрение организационно-технических решений, позволяющих устранить выявленные несоответствия и подготовиться к проведению сертификационного аудита на соответствие системы ИБ требованиям PCI DSS;
- сертификацию на соответствие требованиям PCI DSS.

При проведении предварительного и сертификационного аудита Digital Security выступает в качестве аудитора и консультанта по вопросам ИБ, а LETA IT-company – в качестве консультанта по организационно-техническим аспектам внедрения. В ходе внедрения компания Digital Security участвует вместе с заказчиком в процедурах промежуточного контроля. Такое сочетание централизации ответственности, разделения функций и интеграции рабочих процедур позволяет заказчикам быть уверенными, что проверка созданной системы ИБ на соответствие положениям стандарта будет максимально объективной, а не станет реализовываться по принципу формального подтверждения качества работы одного подразделения другим. Чтобы выполнить эти условия, компании LETA и Digital Security в сентябре 2009 года сформировали консорциум, разработали регламенты совместной работы и внедрили все процедуры взаимодействия.

Предпосылки и преимущества консорциума

Созданию нового бизнес-направления LETA IT-company предшествовала значительная подготовительная работа. В течение полутора лет компания целенаправленно наращивала компетенции по ИБ в финансовом секторе, причем значительные усилия были сконцентрированы именно на внедрении стандартов и требований нормативной базы. С начала 2008 года компания LETA участвовала в проектах подготовки к сертификации в качестве эксперта и исполнителя работ по внедрению организационно-технических решений, устраняющих проблемы, выявленные в ходе предварительного аудита. В частности, был разработан пакет услуг по реализации требований стандарта PCI DSS и внедрению необходимых средств защиты. Этот опыт был использован при формировании полного пакета услуг в сфере PCI DSS.

Важным этапом работы с финансовым сектором стало и вступление компании LETA в сообщество ABISS (Association for Banking Information Security Standards) в июле 2009 года.

Услуги в области PCI DSS в рамках консорциума LETA IT-company и Digital Security существенно расширяют спектр предложений LETA для финансовых структур, а также усиливают концентрацию компетенций компании в профильной сфере ИБ. Создание бизнес-направления PCI DSS стало очередным шагом в реализации стратегии компании LETA по поддержке внедрения в российских организациях важнейших отраслевых и универсальных стандартов в сфере ИБ – российских и международных.

Консалтинговая компания IDS Scheer

Консалтинговая компания IDS Scheer — мировой лидер на рынке инструментальных средств управления бизнес-процессами, решений и услуг в сфере BPM для корпораций и общественных организаций.

Обслуживая более 7000 клиентов в более чем 70 странах, IDS Scheer базирует свою деятельность на инновационных разработках. Компания была основана в 1984 году действующим главой наблюдательного совета и главным советником по техническим вопросам, академиком, доктором Августом-Вильгельмом Шеером (August Wilhelm Scheer), которого многие называют отцом-основателем науки об управлении бизнес-процессами.

Партнерство компаний LETA IT-company и IDS Scheer позволяет при внедрении решений в области ИБ использовать бизнес-ориентированный подход. В основе подхода к реализации процессов ИБ лежат решения по управлению бизнес-процессами. Мы используем мировой опыт крупнейшей консалтинговой компании в области бизнес-процессов и применяем его для решений в области ИБ. При использовании линейки продуктов компании IDS Scheer происходит снижение рисков проекта.

Перед внедрением процессов ИБ производится их проектирование и анализ ключевых моментов работы, принимаются решения о том, каким образом процессы будут работать. На этапе проектирования процессов будут выявлены недочеты, «узкие места» и определены точки в процессе, где не хватает или наоборот есть избыток ресурсов. При моделировании процесса можно проанализировать, насколько внедрение процесса будет экономически эффективно и оправдано в организации. Все это дает возможность выявлять проблемные места уже на этапе проектирования, что позволяет исправить их с наименьшими затратами: изменить внедренную систему сложно, изменить спроектированную модель значительно проще и дешевле.

Консалтинговая компания Cleverics

Cleverics — компания, которая помогает применять возможности информационных технологий с пользой, рационально, с минимальными рисками.

Консорциум создан на стыке сфер ИБ и ИТ, в которых, соответственно, специализируются компании, с целью предоставления заказчикам LETA и Cleverics профессиональных услуг в смежных зонах, выходящих за рамки профильных для LETA IT-company и Cleverics направлений, но логично продолжающих их и дополняющих друг друга.

На сегодняшний день выстраивание процессов ИБ в рамках комплексных консалтинговых проектов (например, проектов построения СУИБ в соответствии со стандартом ISO 27001, выполнения требований других стандартов ИБ и т.д.) предполагает сквозной охват инфраструктуры заказчика и затрагивает ряд смежных процессов, управляемых на другом уровне — управления ИТ. Так, процесс управления инцидентами, выполняющийся в подразделении ИТ, должен иметь четкую связь с инцидентами, выявленными специалистами служб информационной безопасности, выдвигающими требования к регистрации событий и принимающими участие в их обработке, в дальнейшем проводится службами ИТ через традиционные системы управления ИТ — например, Service Desk. Аналогичным образом процессы управления конфигурациями и ИТ-активами ИБ и ИТ стыкуются при реализации ряда других процессов информационной безопасности.

В рамках консорциума LETA IT-company и Cleverics расширят для заказчиков «горизонт покрытия» выстраиваемых процессов, предложат квалифицированное «продолжение» проектов в соседствующие области (для LETA — в ИТ, для Cleverics — в ИБ), обеспечат профессиональную интеграцию задач ИБ и ИТ между собой на прикладном уровне. Опираясь на свои знания и опыт, мы помогаем своим заказчикам спланировать ИТ-стратегию, построить или скорректировать процессы управления ИТ, решить задачи по передаче тех или иных функций управления ИТ на аутсорсинг, а также обеспечить вопросы информационной безопасности при стратегическом планировании. Мы можем организовать сервисную службу (Service Desk) и службу технической поддержки (Help Desk).

Привлечение Cleverics позволит LETA IT-company предлагать клиентам комплексный проект, сразу покрывающий помимо задач и процессов ИБ различные аспекты процессного управления ИТ-деятельностью (от организации взаимодействия с конечными пользователями до процесса управления финансами) и сервисного подхода, лежащего в основе библиотеки ITIL (IT Infrastructure Library — передового опыта управления ИТ) и концепции ITSM (IT Service Management). Клиентам Cleverics привлечение LETA IT-company даст возможность обеспечить бесшовную интеграцию выстроенных процессов управления ИТ с процессами управления ИБ.

LETA IT-company входит в состав
LETA Group – компании №1
по объему продаж на российском
рынке продуктов и услуг в сфере
информационной безопасности по
данным рейтинга «CNews Security
2009: Крупнейшие ИТ-компании
России в сфере защиты
информации»



LETA Group – управляющая компания в сфере передовых информационных технологий

В областях, в которых сейчас работают компании группы, они всегда входят в десятку лучших, по оценкам независимых аналитиков.

В рейтинге CNews Security 2009 LETA Group заняла лидирующие позиции по объему продаж на российском рынке продуктов и услуг в сфере информационной безопасности.

Основной задачей Группы компаний LETA является обеспечение успешного развития и совместного функционирования компаний, входящих в состав Группы.

Функции LETA Group:

- инвестиционная деятельность;
- финансово-экономическое регулирование;
- юридическая поддержка и координация;
- управление информационными технологиями;
- управление новыми проектами;
- координация маркетинга и общественных связей;
- безопасность.

Основная функция LETA Group - инвестиционная деятельность. Инвестиционная стратегия LETA Group основывается на создании, приобретении и управлении активами в различных сегментах российского ИТ-рынка. Они должны обладать значительным потенциалом роста и возможностями для дальнейшей консолидации. Инвестирование происходит только в те проекты, в которых существует потенциальная возможность повышения стоимости активов.

Стратегическая задача LETA Group - создание и развитие лидеров в выбранных областях деятельности, открытие новых путей продвижения бизнеса.

LETA Group – это компания-консолидатор инновационных идей в сфере ИТ.

Основные принципы работы LETA Group:

- сфокусированность на выбранных секторах ИТ-рынка;
- четкое следование внутренним правилам и принципам ведения бизнеса;
- высокий профессионализм работников;
- прозрачность всех действий для клиентов и партнеров.

Под управлением LETA Group находятся следующие компании:



LETA IT-company – первый российский оператор типизированных ИТ-услуг, обеспечивающий заказчикам комплексные решения в области информационной безопасности. Компания предлагает развернутую линейку услуг и решений, закрывающую для клиентов большую часть аспектов современной информационной безопасности.



Компания АСК специализируется на услугах и решениях в сегментах «Промышленная автоматизация» и «Инфраструктурные ИТ-решения», где занимает лидирующие позиции по России. АСК поставляет продукты для автоматизации государственного и муниципального хозяйства, металлургии, машиностроения и энергетики.



Компания «АСКОМ-строй» образована в 2006 году, оказывает полный комплекс работ, связанных с исполнением инженерных подрядов на объектах: от разработки проектной и рабочей документации, поставки оборудования, проведения пусконаладочных работ до сдачи систем в эксплуатацию и последующего гарантийного обслуживания.



ДАМАСК – российский разработчик одноименной системы электронной очереди. Компания выросла из направления электронных очередей ООО «Группа компаний АСК», которое с 2004 года занималось разработкой и внедрением продукта в государственных и коммерческих структурах Свердловской области.



ЗАО «ИСЕТ» обладает эксклюзивными правами в странах СНГ на все продукты компании ESET – международного разработчика программного обеспечения в области информационной безопасности. ESET предлагает интеллектуальные решения для домашних и корпоративных пользователей, гарантирующие защиту отдельных компьютеров и элементов компьютерных сетей от угроз, связанных с вредоносными программами.



MrSoft – интернет-магазин лицензионного программного обеспечения и игровых приложений. На сегодняшний день ассортимент магазина насчитывает более 5000 наименований, представленных сотнями производителей, и этот список постоянно обновляется и расширяется.



Компания «ГК АСК» образована на базе одного из крупнейших системных интеграторов Уральского региона ООО «Группа компаний АСК», работающего на ИТ-рынке с 1995 г.

Весной 2010 г. было объявлено о новой стратегии «ГК АСК». Со второго квартала 2010 года компания запускает продуктовую модель бизнеса и становится российским разработчиком программного обеспечения на рынке промышленной автоматизации.

При разработке своего продуктового портфеля «ГК АСК» сконцентрировала усилия на направлении, находящемся на стыке таких областей, как прогнозирование, контроль качества и безопасность.

Кроме того, новые продукты «ГК АСК» позволяют эффективно решать такие важнейшие для большинства российских предприятий практические задачи, как минимизация издержек, связанных с выпуском некачественной продукции, и оптимизация планов модернизации производственной базы – с учетом степени износа оборудования и реальных финансовых возможностей предприятия.

В первую очередь «ГК АСК» продвигает линейку специализированных продуктов, которые позволяют:

- организовать сбор, хранение и визуализацию данных о ходе технологических процессов;
- своевременно выявлять выход технологического процесса за допустимые границы;
- вести журнал фактических причин нештатных ситуаций и работ по их устранению, ускоряющий поиск решений при повторном возникновении сходных инцидентов;
- оптимально перенастраивать технологические процессы при нештатных ситуациях;
- прогнозировать появление брака; имитировать инциденты в технологических процессах при обучении специалистов перед их выходом на реальное производство.

Продуктовая стратегия «ГК АСК» имеет следующие особенности:

1. Компания изначально ориентируется на то, что потребности российских предприятий будут динамично меняться по мере выхода из кризиса отдельных отраслей и экономики в целом. Соответственно, «ГК АСК» использует адаптивную технологию разработки, вывода на рынок новых и развития существующих продуктов.
2. При формировании продуктового портфеля компания намерена упрощать функциональность конкретных продуктов до уровня, позволяющего резко снизить затраты на разработку и внедрение, «закрыв» при этом до 80% потребностей Заказчика.

Новая стратегия «ГК АСК» предусматривает также сохранение и развитие традиционного для компании проектного бизнеса в сфере промышленной автоматизации. За 15 лет работы «ГК АСК» стала одним из признанных лидеров российского рынка в этом сегменте, выполнила десятки инновационных проектов для предприятий, работающих в машиностроении, электроэнергетике, горнодобывающей промышленности, госсекторе и др. Среди клиентов «ГК АСК» такие крупнейшие предприятия, как «Уралвагонзавод», Виз-Сталь, НТМК, Уральский турбинный завод, ВСМПО-АВИСМА и др. Появление у «ГК АСК» собственного продуктового портфеля позволит еще больше усилить проектное направление, прежде всего за счет дополнительных компетенций, расширения консалтинговой составляющей, а также снижения себестоимости благодаря частичному замещению уникальных разработок типизированными продуктами и услугами.



Компания «АСКОМ-строй» образована в 2006 году. До 2009 года существовала как строительно-монтажное подразделение в рамках одного из крупнейших системных

интеграторов Уральского региона ООО «Группа компаний АСК». В 2010 году выделена в самостоятельное бизнес-направление.

Компания предлагает полный комплекс работ, связанных с исполнением инженерных подрядов на объектах: от разработки проектной и рабочей документации, поставки оборудования, проведения пусконаладочных работ до сдачи систем в эксплуатацию и последующего гарантийного обслуживания.

Компания располагает штатом квалифицированных специалистов в областях электромонтажа, монтажа систем охранно-пожарной сигнализации, контроля доступа, видеонаблюдения, построения структурированных кабельных сетей (СКС) и волоконно-оптических линий связи (ВОЛС).

Компания «АСКОМ-строй» обладает набором лицензий, позволяющих производить необходимые Заказчикам работы:

1. Лицензия МЧС от 5 октября 2007 г. № 1/11846 на осуществление деятельности по тушению пожаров: выполнение проектных работ по средствам обеспечения пожарной безопасности зданий и сооружений.
2. Лицензия МЧС от 5 октября 2007 г. № 2/21530 на осуществление производства работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений.
3. Свидетельство от 10 марта 2010 г. № 230 о допуске СРО «Гильдия строителей Урала» к видам работ по строительству, реконструкции, капитальному ремонту объектов капитального строительства, которые оказывают влияние на безопасность объектов капитального строительства.
4. Лицензия Управления ФСБ России от 22 июля 2009 г. № 2168 на осуществление работ с использованием сведений, составляющих государственную тайну.

Направления деятельности компании «АСКОМ-строй»:

- **построение дата-центров:**
 - строительство серверных и кроссовых помещений «под ключ»;
 - создание мобильных дата-центров;
- **создание инженерно-технических систем защиты периметров объектов:**
 - охранное видеонаблюдение;
 - периметральная охранная сигнализация;
 - системы контроля доступа, управление доступом;
- **создание инженерной инфраструктуры зданий и сооружений:**
 - построение СКС, ВОЛС;
 - все виды электромонтажных работ;
 - построение систем пожарной сигнализации оповещения при пожаре и автоматического пожаротушения.



Компания «ДАМАСК» является производителем одноименной системы управления очередями. Всего в 2009 году на базе системы «ДАМАСК» было автоматизировано более 2150 рабочих мест, при этом на ее основе недавно была

внедрена одна из самых больших в мире систем электронных очередей. Компания «ДАМАСК» является крупнейшим в России производителем аппаратно-независимой системы электронной очереди.

Система «ДАМАСК» — одна из старейших на российском рынке и наиболее функциональных систем управления очередями.

Её отличает независимость от аппаратной платформы, широкие возможности автоматизации процедур, а также эффективная работа в режиме крупной территориально-распределенной системы. При этом в «ДАМАСК» полностью поддерживаются все современные и наиболее эффективные приемы работы с посетителями, а также алгоритмы управления очередями, оптимизации использования рабочих мест, нагрузки на специалистов и общей продолжительности обслуживания посетителей.

«ДАМАСК» имеет развитые средства автоматизации процедур и интеграции с системами CRM и другими элементами корпоративной ИС, а также проработанные средства решения задач, связанных с информационной и физической безопасностью фронт-офиса. Еще одной особенностью системы является гибкое конфигурирование. Заказчик может самостоятельно перенастраивать перечни услуг, списки и специализацию операционистов, алгоритмы автоматизации различных операций, состав рабочих мест, характер отображаемой информации и другие параметры системы.

Основные возможности системы электронной очереди «ДАМАСК»

- **Регистрация и управление обслуживанием клиента**

Система «ДАМАСК» полностью поддерживает сложные схемы регистрации клиента в очереди на получение необходимого набора услуг. При этом система управления очередью автоматически упорядочивает операции обслуживания клиента конкретными специалистами в соответствии с заданными технологическими картами, учитывает расписание и доступность специалистов, автоматически модифицирует процедуры обслуживания с учетом категории (например, Gold, VIP и др.) и статуса клиента (в т.ч. вычисленного на основе имеющейся информации о нем). Обслуживание клиента можно приостанавливать и возобновлять после взятой паузы; уже в ходе обслуживания клиента список заказанных им услуг может корректироваться, это не требует получения дополнительного талона. Система управления очередью «ДАМАСК» поддерживает предварительную запись (в т.ч. через Интернет) с выбором дня и желаемого времени приема, поддерживается режим «живой очереди» и резервирование части талонов для выдачи только в день обращения.

- **Расширенное управление расписаниями**

Для каждой услуги и в целом для организации можно задавать приемные дни и часы, технологические и иные перерывы, особенности графика в праздничные и выходные дни, численность закрепленного за услугой персонала. Также в расписании можно задавать часы приема конкретных специалистов, а также фиксировать нормативы времени, необходимого для оказания каждой операции. Вся эта информация используется алгоритмами распределения посетителей и оптимизации работы фронт-офиса.

- **Оперативная оптимизация работы фронт-офиса**

Система управления очередью «ДАМАСК» обеспечивает полный онлайн-контроль и удаленное управление работой офисов обслуживания с рабочего места сотрудника, имеющего соответствующий уровень прав. Система автоматически оповещает о критических событиях, например, о превышении оператором установленного времени обслуживания клиента или увеличении средней продолжительности ожидания в очереди к определенной категории специалистов. Набор отслеживаемых параметров и критические области для их значений задаются настройками.

Еще один механизм позволяет оперативно переключать конфигурации системы по заданным сценариям в зависимости от фактической динамики очередей, а также плановых изменений уровня спроса на пакеты услуг (например, наивысший спрос на определенные услуги может приходиться на определенное время дня, день недели или месяца). Такое переключение приводит к одномоментному согласованному изменению множества параметров системы, например числа рабочих мест и распределения услуг по ним, нормативов приема посетителей и др.

- **Управление отображаемой информацией**

Специальное ПО, поставляемое в составе системы, обеспечивает заказчику полный контроль за составом и видом информации, отображаемой на пультах выбора услуг, на информационных табло и в талонах. Отметим, что наряду с базовой информацией (номером очереди, датой и временем выдачи талона) на талоне можно распечатывать большой объем дополнительных данных, включая список выбранных услуг, планируемое время вызова (рассчитывается системой в зависимости от текущего состояния очередей, набора услуг, статуса клиента, нормативов и реальной статистики обслуживания). На информационные табло можно выводить текстовую и графическую информацию, бегущую строку и видеоролики. Предусмотрено гибкое управление рекламным и информационным мультимедийным контентом, а также настройка параметров изображений в соответствии с фирменным стилем организации. Все это позволяет эффективно использовать электронную очередь при проведении маркетинговых программ.

В 2009 году выпущена новая версия (3.1) технологической платформы «ДАМАСК», в которой значительно расширены возможности масштабирования и централизованного управления, внедрены особые технологии создания отраслевых решений, расширена функциональность уже имеющихся блоков системы. Отметим несколько наиболее важных нововведений.

В новой версии «ДАМАСК» полностью сняты ограничения по выбору аппаратного обеспечения системы электронной очереди. Наряду с обычным офисным оборудованием (LCD-мониторы, плазменные и ЖК-телевизоры, информационные киоски), в качестве компонент системы теперь можно использовать всевозможные специализированные устройства, например, светодиодные и сегментные табло, аппаратные пульта операторов, выпускаемые другими фирмами-производителями систем электронных очередей. Это позволяет с максимальным сохранением произведенных инвестиций проводить модернизацию уже установленных систем электронной очереди, заменяя софт на ПО «ДАМАСК».

В 2009 году система управления очередью «ДАМАСК» пополнилась модулем расширенного управления расписаниями с практически неограниченными возможностями конфигурирования графика оказания услуг. В составе системы появились модуль оценки посетителями качества обслуживания и модуль централизованного сбора статистики. При этом совокупность оценок качества используется при построении отчетов, анализе и формировании эффективных мотивационных схем. Модуль статистики обеспечивает сбор и консолидацию информации о работе всех элементов территориально распределенной системы, формирование сводок и отчетов информационной поддержки управленческих решений с пошаговой детализацией (drill-down) – вплоть до просмотра журнала обработки каждого талона. В новой версии системы «ДАМАСК» появились мощные инструменты удаленной записи через Интернет (с использованием ПК, мобильных телефонов, смартфонов и коммуникаторов).

В настоящее время платформа «ДАМАСК» широко используется для создания территориально распределенных систем электронной очереди. Улучшение поддержки такого режима работы – это важнейшее направление развития системы «ДАМАСК». В частности, предусмотрено создание в 2010 году подсистемы централизованного управления локальными системами в территориально распределенных структурах.

Другой важнейшей задачей является упрощение интеграции системы электронных очередей с другими элементами информационной инфраструктуры на объектах заказчика. Соответственно, система «ДАМАСК» будет развиваться в направлении создания унифицированных открытых протоколов взаимодействия с другими информационными системами.

В 2009 г. была создана линейка специализированных отраслевых решений. В отличие от базовой версии конфигурация таких решений учитывает специфику работы организации/учреждения конкретной отрасли. В настоящее время создано пять таких решений: для кредитных организаций («ДАМАСК-Банк»), для многофункциональных центров оказания услуг населению («ДАМАСК-МФЦ»), для структур Федеральной миграционной службы («ДАМАСК-ФМС»), для ГИБДД («ДАМАСК-МРЭО») и для поликлиник («ДАМАСК-МЕД»). Завершается разработка решений для страхового бизнеса («ДАМАСК-СК»), для офисов обслуживания телекоммуникационных операторов («ДАМАСК-телеком»). Идут работы по созданию специализированного решения для пенсионных фондов.



Компания ESET (www.esetnod32.ru) — международный разработчик антивирусного программного обеспечения и решений в области компьютерной безопасности для корпоративных и домашних пользователей — была основана в 1992 году. Штаб-квартиры ESET находятся в г. Братиславе (Словакия) и в г. Сан-Диего (США).

Компания представлена в более чем 160 странах мира. ESET является пионером в области создания эвристических методов обнаружения угроз, которые позволяют детектировать и обезвреживать как известные, так и новые вредоносные программы.

Российское представительство ESET открылось в январе 2005 года и входит в тройку стратегически важных представительств компании в мире. Российское представительство ESET курирует продвижение и продажу программного обеспечения ESET во всех странах СНГ. По данным исследовательских компаний КОМКОН и «Ромир», ESET NOD32 является вторым по популярности антивирусным решением в России и защищает каждый третий компьютер. При этом 90% пользователей рекомендуют продукты ESET NOD32 своим друзьям и знакомым.

Антивирусные решения ESET, выпускаемые под брендом ESET NOD32, удостоились рекордного количества наград «VB100», выданных по результатам тестирования британского журнала Virus Bulletin. Антивирус ESET NOD32 назван лучшим продуктом 2006 и 2007 года австрийской тестовой лабораторией Андреаса Клименти AV-Comparatives и является абсолютным победителем в номинациях «Проактивность», «Минимальное количество ложных срабатываний», «Скорость сканирования» и «Детектирование полиморфных вирусов». В России решения ESET сертифицированы ФСТЭК России и рекомендуются для использования в информационных системах персональных данных до класса К1 включительно.

Партнерская сеть российского представительства ESET включает три компании-дистрибьютора («1С», MONT, RRC) и свыше 300 компаний-партнеров, которые осуществляют конечные продажи продуктов ESET NOD32. Более 70 из них имеют статус Premier Partner. Партнерская сеть охватывает 90 городов России. Партнеры компании тесно взаимодействуют с ESET, что позволяет оперативно и своевременно реагировать на запросы клиентов. Антивирусные решения ESET NOD32 доступны в любой точке России и практически в любой стране мира.

Клиентами ESET в России и странах СНГ являются крупные российские и международные компании:

ОАО «Газавтоматика», Газпром-Медиа, ООО «Газпром Добыча Уренгой», ООО «Газпром Трансгаз Кубань», филиал ОАО «ФСК ЕЭС», группа компаний «Евраз», ОАО «Пензенская генерирующая компания», ОАО «Карелэнерго», ОАО «Южная сетевая компания», АО «МОЭК», ОАО «Ингосстрах», группа компаний «Трансас», ООО «РН Архангельскнефтепродукт», ОАО «Московский завод «Кристалл», «Ленгипротранс», «Макслевел», ОАО «Белкамнефть», ООО «РН-СахалинНИПИморнефть», телеканал MTV, АК «Алроса», Министерство юстиции РФ, Администрация города Перми, «Узбектелеком», «Мастер банк», «Международный банк Азербайджана», Восточный экспресс банк, торгово-промышленная группа «Кристалл», МВО-Столица, фирма «1С», News Outdoor Russia, МИСиС, «СИА Интернейшнл ЛТД», Мариинский театр, АО «Хоум Кредит Банк» и другие.



MrSoft (www.mrsoft.ru) – интернет-магазин лицензионного программного обеспечения и игровых приложений с удобной доставкой. Магазин работает как с частными, так и с юридическими лицами.

Постоянно пополняемый ассортимент MrSoft насчитывает более 5000 наименований, представленных сотнями разработчиков.

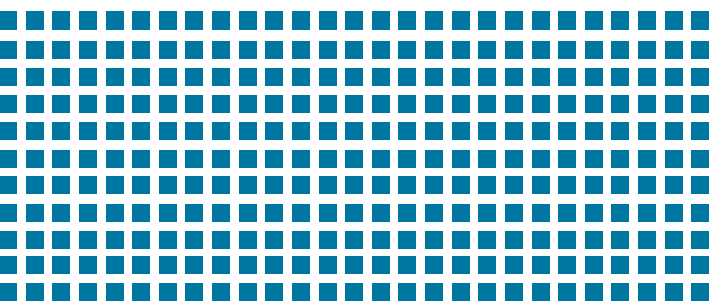
MrSoft ориентируется на максимально полную реализацию потребностей клиентов, что обеспечивает:

- выверенность продуктовой линейки (в ассортименте MrSoft представлены только самые необходимые и востребованные продукты. Компания не перегружает магазин и не создает из него «склад невостребованного ПО»);
- простоту интерфейса поиска и заказа;
- широкие возможности оплаты (большинство из доступных в России – наличные и безналичные платежи, пластиковые карты, банковские переводы, интернет-платежи);
- возможность получить профессиональную персональную техническую консультацию;
- максимальную автоматизацию всех процессов.

Принципы работы позволяют MrSoft существенно снизить затраты на персонал и предлагать продукты по более выгодным потребителям ценам.

Высококвалифицированные специалисты магазина консультируют заказчиков по поводу выбора оптимального продукта, способов оплаты и доставки, оптимизации схемы лицензирования.

MrSoft регулярно проводит исследования рынка лицензионного программного обеспечения, которые помогают компании правильно формировать свои продуктовые предложения. Уникальным преимуществом MrSoft является разработанный показатель MrSoftIndex, демонстрирующий ключевые тенденции на рынке программного обеспечения и игровых приложений и позволяющий точнее предвидеть и эффективнее реализовывать потребности покупателей.



LETA IT-company

109129, Москва, ул. 8-я Текстильщиков, д. 11, стр. 2

Тел./факс: +7 (495) 921 1410

e-mail: info@leta.ru , <http://www.leta.ru>

<http://letablog.livejournal.com/>