



bcc

Информационная безопасность в современной организации

Широкое применение информационных систем в современной организации приводит к экспоненциальному росту угроз информационной безопасности (ИБ).

Найти баланс между эффективностью бизнеса и минимизацией угроз ИБ — технически сложная оптимизационная задача. Она требует комплексного подхода, включающего изменение бизнес-процессов и организационных процедур, внедрение специальных средств защиты информации, модернизацию всех элементов корпоративной информационной системы предприятия в соответствии с требованиями ИБ.



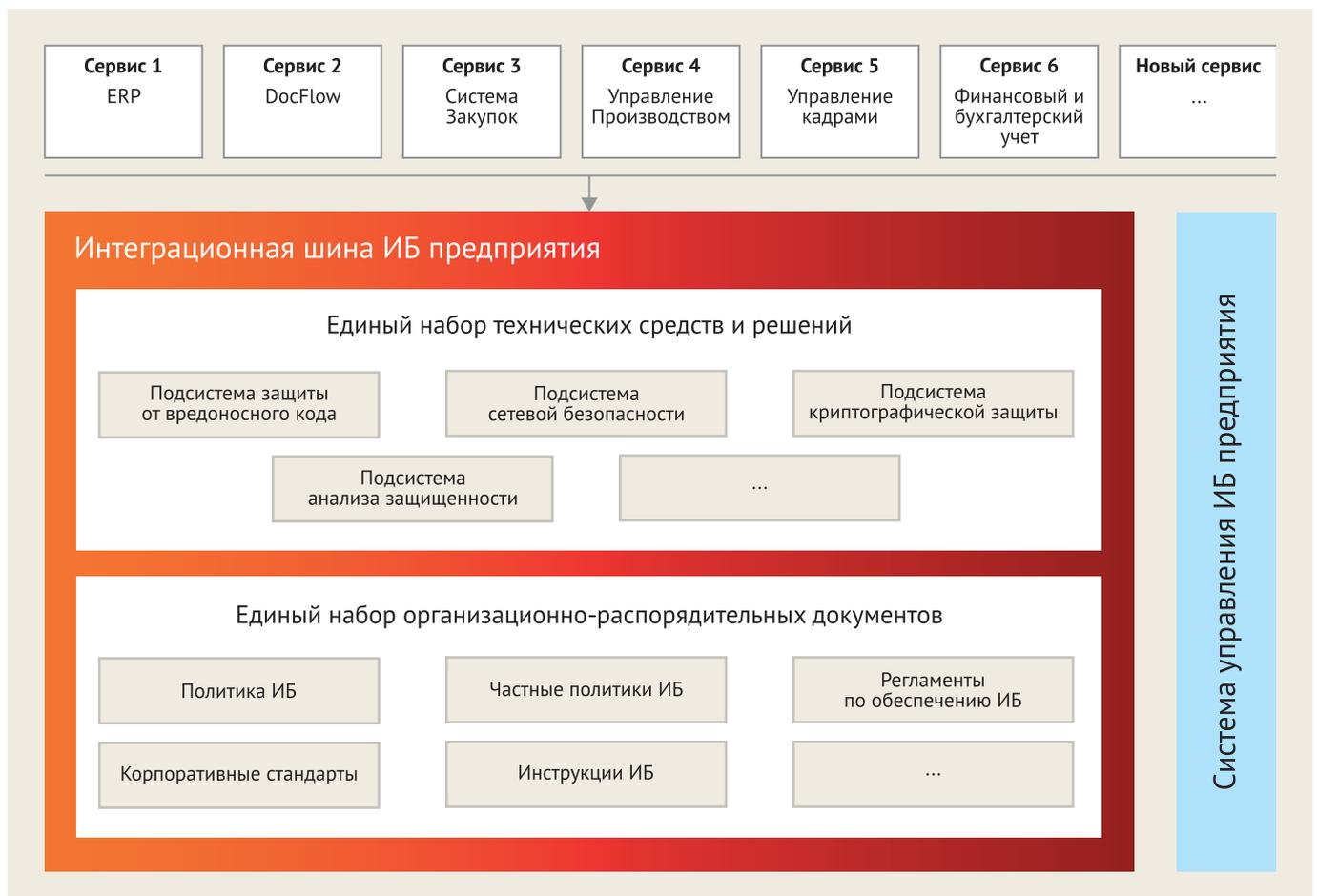
Особенности подхода компании ВСС к вопросам обеспечения информационной безопасности

При построении системы обеспечения информационной безопасности необходимо учитывать следующие факторы:

- существующие ИТ-технологии и их особенности,
- текущие потребности и специфику бизнеса,
- законодательные требования и требования регуляторов,
- перспективы дальнейшего развития бизнеса.

Внедрение комплексных ИТ-решений и систем обеспечения информационной безопасности является одним из основных направлений бизнеса ВСС. В этой области специалисты компании накопили не только значительную технологическую экспертизу, но и большой практический опыт реализации проектов. Для минимизации угроз возникновения инцидентов ИБ и снижения ущерба от действий злоумышленников компания ВСС делает акцент на комплексную защиту, которая охватывает не только критически важные бизнес-процессы, но и все обеспечивающие их работу ИТ-системы и сервисы.

Решения и услуги ВСС в области обеспечения ИБ базируются на использовании методологии **единой шины информационной безопасности**, основополагающие принципы построения которой показаны на схеме:





Преимущества внедрения **единой шины информационной безопасности:**

- Создание многоуровневой, гибкой и масштабируемой системы обеспечения информационной безопасности **всех элементов ИТ-инфраструктуры и сервисов заказчика.**
- Соответствие законодательным, отраслевым и внутрикорпоративным требованиям.
- Унификация принципов, методов и механизмов технической реализации для обеспечения ИБ на всех уровнях иерархии предлагаемого решения.
- Преимущество предлагаемого решения по отношению к существующей системе обеспечения информационной безопасности и стратегии развития ИТ-сервисов заказчика.
- Бесшовная интеграция сервисов по обеспечению ИБ в существующие бизнес-процессы и ИТ-инфраструктуру заказчика.

Комплексный подход компании ВСС, базирующийся на использовании перспективных технологий и продуктов в области информационной безопасности, позволяет предлагать полный спектр услуг: от проведения консалтинга, проектирования архитектуры сложных систем ИБ и запуска их в промышленную эксплуатацию, до технической поддержки внедренных решений и обучения пользователей.

В рамках создания единой шины информационной безопасности заказчика, решения и услуги компании ВСС сгруппированы по следующим направлениям:

- Организационное обеспечение системы ИБ.
- Обеспечение соответствия системы ИБ требованиям регуляторов.
- Построение инфраструктуры ИБ.
- Внедрение средств защиты информации.

Решения и услуги ВСС в области информационной безопасности

Безопасность!

Организационное обеспечение системы ИБ

Основополагающими причинами, обуславливающими возникновение инцидентов ИБ, являются следующие факторы:

- изначально не были сформулированы принципы обеспечения ИБ в организации;
- не формализованы требования к процессам ее обеспечивающим;
- не регламентирован порядок и правила их выполнения и развития.

Как результат, система ИБ строится по принципу нейтрализации уже произошедших инцидентов, мероприятия по обеспечению безопасности не носят превентивного характера, не скоординированы по месту и времени, а различный уровень квалификации персонала оказывает негативное влияние на конечный результат.

Именно поэтому компания ВСС рассматривает услуги по организационному обеспечению системы ИБ как важнейшую составную часть комплексной системы противодействия информационным угрозам в компаниях и организациях.

Решение ВСС для организационного обеспечения системы ИБ состоит из следующих услуг:

- разработка Концепции ИБ,
- разработка Политик ИБ,
- разработка корпоративных стандартов по ИБ.

Концепция ИБ Компании

При разработке Концепции ИБ компании специалисты ВСС определяют основные цели и задачи защиты, методы достижения требуемого уровня безопасности информации в организации и предоставляют не только обобщенное описание объектов защиты, но и принципы контроля эффективности системы ИБ.

Политики ИБ Компании

Комплект Политик ИБ, разрабатываемых специалистами ВСС, позволяет конкретизировать требования по обеспечению информационной безопасности в рамках выделенных процессов или информационных подсистем, полностью регламентирует все необходимые процедуры проектирования, внедрения и дальнейшей поддержки систем ИБ и четко прописывает распределение обязанностей и ответственности сотрудников заказчика за обеспечение информационной безопасности.

Корпоративные стандарты по ИБ

Компания ВСС предлагает свои услуги по разработке корпоративных стандартов по ИБ для внедрения системного подхода к защите информации в рамках всей компании, построению целостной и эффективной системы обеспечения и управления ИБ, поддержанию необходимого уровня защищенности всех информационных активов (ИТ-системы, бизнес-приложения, сервисы и т. д.) по единым принципам.

Бизнес-преимущества услуг:

- Повышение эффективности взаимодействия между участниками работ по обеспечению ИБ.
- Повышение защищенности бизнес-процессов и информационных активов организации.
- Снижение ущерба от возможных инцидентов ИБ.

Примеры реализованных проектов:

Международная промышленная компания: «Формализация требований к обеспечению ИБ».

В рамках решения данной задачи специалистами ВСС была определена модель угроз и нарушителя, разработана Концепция ИБ Компании, а также конкретизированы требования (частные Политики ИБ) по обеспечению ИБ для определенных заказчиком критичных процессов/информационных систем.

Обеспечение соответствия системы ИБ требованиям регуляторов

При решении вопросов в области обеспечения ИБ, ответственное подразделение организации нередко сталкивается с тем, что при реализации проектов необходимо учитывать требования многих сторон.

Помимо требований бизнес-подразделений компании и головного офиса, в последнее время становятся все более актуальными требования различных регуляторов (Центральный банк РФ, ФСБ России, ФСТЭК РФ и т. д.).

Для приведения процесса обработки информации ограниченного доступа в соответствие установленным и принятым требованиям, практикам и нормам по защите информации компания ВСС предлагает следующие услуги:

- Обеспечение соответствия требованиям стандарта Банка России СТО БР ИББС-1.0-2008.
- Обеспечение соответствия требованиям стандарта индустрии платежных карт (PCI DSS).
- Обеспечение соответствия требованиям Федерального закона № 152-ФЗ «О персональных данных».
- Обеспечение соответствия требованиям BS ISO/IEC 27001.
- Построение комплексной системы защиты конфиденциальной информации.

Бизнес-преимущества услуг:

- Снижение рисков возникновения санкций со стороны органов, осуществляющих контроль в области соблюдения требований по обеспечению безопасности информации.
- Снижение ущерба от возможных инцидентов ИБ.
- Повышение доверия клиентов и партнеров к организации.

Примеры реализованных проектов:

Крупная телекоммуникационная компания: «Приведение обработки персональных данных в соответствие требования Федерального закона № 152-ФЗ "О персональных данных"».

В рамках данного проекта специалистами ВСС были проведены следующие работы:

- определены процессы обработки персональных данных (ПДн) и сформированы требования к их защите в соответствии с актуальными угрозами, определенными в рамках документа «Модель угроз»;
- спроектировано и внедрено комплексное техническое решение, нейтрализующее актуальные угрозы ИБ;
- проведено необходимое обучение сотрудников заказчика по вопросам защиты ПДн;
- разработан необходимый комплект организационно-распорядительной документации по вопросам обработки и защиты ПДн в соответствии с требованиями регулирующих органов и законодательных актов.



Построение инфраструктуры обеспечения ИБ

Типовая модель современной компании имеет, как правило, территориально-распределенную организационную структуру со значительным количеством информационных активов и автоматизированных бизнес-процессов в каждом подразделении.

Одной из важнейших задач обеспечения ИБ для такой компании является построение комплексной инфраструктуры обеспечения информационной безопасности, способной не только эффективно противостоять угрозам ИБ, но и минимизировать возможность доступа злоумышленников к критически важным приложениям и конфиденциальным данным.

Решение ВСС в области построения инфраструктуры обеспечения ИБ состоит из следующих услуг:

- Построение центра управления инфраструктурой ИБ.
 - Построение комплексной системы сетевой безопасности.
 - Построение системы безопасного удаленного взаимодействия (доступа к сервисам).
 - Построение корпоративной системы анализа защищенности сетевой инфраструктуры.
 - Построение системы контроля неизменности сетевой инфраструктуры.
 - Построение корпоративной системы защиты каналов связи.
 - Построение системы контроля соответствия корпоративной политике ИБ.
 - Построение системы защиты конфиденциальных переговоров.
 - Построение корпоративной системы защиты от утечек конфиденциальной информации (DLP).
 - Построение корпоративной системы защиты от вредоносного кода.
 - Построение системы защиты виртуальной инфраструктуры.
 - Построение системы защиты баз данных.
 - Построение корпоративной системы экстренного уничтожения информации.
- Построение инфраструктуры PKI.
 - Помощь заказчику в устранении инцидентов ИБ.
 - Тестирование на проникновение.

Примеры реализованных проектов:

Крупная торговая организация:
«Построение системы безопасного удаленного взаимодействия».

В рамках решения данной задачи специалистами ВСС были выполнены следующие виды работ:

- определены типовые роли удаленных пользователей системы и соответствующий для каждой роли необходимый набор ресурсов/сервисов информационной системы организации;
- изучена информационная инфраструктура заказчика;
- выполнены все необходимые работы по проектированию и внедрению технического решения на базе продуктов компании Stonesoft Corporation (StoneGate SSL VPN, StoneGate Firewall/VPN, StoneGate Management Center);
- разработан комплект организационно-распорядительной документации, описывающий порядок и правила эксплуатации системы, а также частная Политика ИБ по обеспечению защищенного удаленного взаимодействия.

Бизнес-преимущества услуг:

- Снижение ущерба от возможных инцидентов ИБ.
- Создание предпосылок для выполнения требований регулирующих органов, осуществляющих контроль в области соблюдения требованиям по обеспечению безопасности информации.

Внедрение средств защиты информации

Как правило, система защиты, созданная несколько лет назад, уже не обеспечивает необходимый для организации уровень безопасности ее систем, бизнес-процессов и информации. Это обусловлено разными причинами, среди которых можно отметить:

- Появление новых или изменение существующих угроз ИБ.
- Изменение бизнес-процессов и информационных систем в организации.
- Изменение аппаратной, программной, системной составляющей информационных систем организации.
- Изменение масштабов организации.

Каждая из вышеперечисленных причин приводит к тому, что подразделение организации, отвечающее за обеспечение ИБ, вынуждено внедрять соответствующие системы безопасности или корректировать ранее внедренные механизмы защиты в рамках определенных бизнес-процессов или информационных систем.

Компания ВСС предлагает следующие услуги по выполнению данной задачи:

- Внедрение средств межсетевого экранирования.
- Внедрение средств защиты от несанкционированного доступа (НСД).
- Внедрение средств защиты от вредоносного кода.
- Внедрение средств криптографической защиты.
- Внедрение средств обнаружения и предотвращения вторжений.
- Внедрение средств анализа защищенности.
- Внедрение средств защиты от спама.

Бизнес-преимущества услуг:

- Снижение ущерба от возможных инцидентов ИБ.

Примеры реализованных проектов:

Крупный банк, входящий в ТОП-10: «Внедрение средств обнаружения и предотвращения вторжений».

В рамках данного проекта специалистами ВСС были проведены работы по обследованию сегмента защищаемой инфраструктуры и внедрению средств обнаружения и предотвращения вторжений на базе оборудования компании Cisco Systems (Cisco ASA 5540 с модулем ASDM).

Управляющая компания крупного строительного холдинга: «Внедрение средств защиты от несанкционированного доступа и анализа защищенности».

В рамках этого проекта специалистами ВСС, совместно с экспертами заказчика, были выполнены следующие работы:

- Разработаны и внедрены комплексные технические решения по защите рабочих мест сотрудников компании от несанкционированного доступа и копирования на внешние носители информации. Основу решения составили продукты компаний SecurIT (Zlock), RSA, The Security Division of EMC (RSA SecurID) и Max Patrol (Positive Technologies).
- Проведена оценка уязвимостей прикладного и системного программного обеспечения и предложен комплекс мер, направленный на превентивное устранение угроз ИБ.



Почему ВСС

- Обширный опыт построения ИТ-инфраструктуры различного масштаба и сложности, включая реализацию комплексных проектов по ИБ.
- Большой опыт проведения работ в соответствии с требованиями регулирующих органов (ФСБ и ФСТЭК России).
- Наличие необходимых лицензий для выполнения работ по защите информации ограниченного доступа (ПДн, конфиденциальная информация).
- Широкая отраслевая экспертиза.
- Индивидуальный подход к каждому Заказчику, учитывающий специфику его бизнеса.
- Развитая филиальная сеть, расположенная в крупных регионах России.

Наивысшие статусы Компании

- Stonesoft Corporation — Expert Partner;
- Cisco Systems — Gold Partner;
- Microsoft Corporation — Gold Partner;
- Oracle — Platinum Partner;
- Citrix — Platinum Partner;
- VMWARE — Enterprise Partner.

Компания ВСС обладает всеми необходимыми лицензиями для оказания услуг в области информационной безопасности.

Лицензии ФСТЭК России:

- на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации);
- на деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- на проведение работ, связанных с созданием средств защиты информации;
- на деятельность по технической защите конфиденциальной информации.

Лицензия Министерства Обороны РФ:

- на осуществление деятельности в области создания средств защиты информации.

Лицензии ФСБ России:

- на осуществление работ с использованием сведений, составляющих государственную тайну;
- на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем;
- на распространение шифровальных (криптографических) средств;
- на осуществление технического обслуживания шифровальных (криптографических) средств.

Применяемые технологии и продукты

Средства защиты от несанкционированного доступа (НСД): Cisco Systems; Microsoft; HyTrust, Inc.; компания SecurIT; Aladdin Security Solutions; ГК «Информзащита»; компания «Физтех-софт».

Средства усиленной аутентификации: RSA, The Security Division of EMC; Aladdin Security Solutions.

Средства защиты от вредоносного кода: Microsoft; ЗАО «Лаборатория Касперского»; ООО «Доктор Веб»; Symantec; Trend Micro Inc.; ESET; LLC.; McAfee.

Средства шифрования (дисков, папок): Aladdin Security Solutions; компания SecurIT.

Межсетевые экраны (Firewall): Cisco Systems, Inc.; Microsoft; Check Point Software Technologies Ltd.; ESET; LLC.; Stonesoft.

Средства анализа защищенности (СУБД, приложения, ОС и т.д.): Oracle; Application Security, Inc.; Imperva.

Intrusion Detection System/ Intrusion Prevention System (IPS/IDS): Stonesoft; Cisco Systems, Inc.; CheckPoint Software Technologies; Reflex Security; Catbird Networks.

Virtual Private Network (VPN): Cisco Systems; CheckPoint Software Technologies; Stonesoft; ГК «Информзащита»; ОАО «ИнфоТеКС»; ООО «АМИКОН».

Secure Sockets Layer VPN (SSL VPN): Cisco Systems; Stonesoft; Check Point Software Technologies Ltd.

Public Key Infrastructure (Инфраструктура PKI): Microsoft; RSA; The Security Division of EMC.

Удостоверяющие центры: ЗАО «Сигнал-КОМ»; ООО «Крипто-Про».

Средства анализа защищенности: Positive Technologies; Qualys, Inc.; Outpost24.

Средства контроля соответствия (Compliance appliance): Cisco Systems; Symantec; IBM Tivoli software; Tripwire, Inc.; Catbird Networks.

Network Access Control (NAC): Cisco Systems; Symantec.

Security Information Manager (SIM): Cisco Systems, Inc.; Symantec; ArcSight; netForensics; Stonesoft; IBM Internet Security Systems; Tripwire, Inc.

Data Leak/Loss Prevention (DLP): Symantec; Websense; McAfee.

Identity & Access Management (IAM): IBM Tivoli software; Oracle.

Information Rights Management (IRM): Microsoft; Oracle.



www.bcc.ru

E-mail: office@bcc.ru

➤ **ВСС Санкт-Петербург**
194100, Россия, г. Санкт-Петербург,
Кантемировская ул., 20
тел.: +7 (812) 327-4444
факс: +7 (812) 327-4337

➤ **ВСС Москва**
123022, Россия, г. Москва,
Звенигородское ш., 18/20, стр. 1,
тел.: +7 (495) 258-8100
факс: +7 (495) 258-9908

Региональные офисы:

- Краснодар
- Новосибирск
- Екатеринбург