ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КОНСАЛТИНГОВЫЕ УСЛУГИ

ДиалогНаука

КТО МЫ?

Более 25 лет «ДиалогНаука» является одной из ведущих российских компаний, специализирующихся в области информационной безопасности.

Компания оказывает услуги в области системной интеграции, консалтинга и внедрения комплексных решений по защите информации.

Свою деятельность «ДиалогНаука» осуществляет на основании лицензий ФСБ, ФСТЭК и Министерства обороны РФ.

Компания имеет аккредитации QSA и ASV, позволяющие проводить аудит и ASV сканирования уязвимостей в соответствии с требованиями стандарта PCI DSS.

«ДиалогНаука» является членом АЗИ, АДЭ, НП «АБИСС», АП КИТ, является сертифицированным партнёром BSI Management Systems CIS и имеет свидетельство об аккредитации в области персональных данных от Роскомнадзора.

Система менеджмента качества сертифицирована на соответствие требованиям ISO 9001:2008. Система менеджмента ИБ сертифицирована в соответствии с ГОСТ ИСО 27001.

ЦИКЛ КОНСАЛТИНГОВЫХ УСЛУГ

Для эффективного обеспечения информационной безопасности необходимо применять комплексный подход, предусматривающий применение как организационных, так и технических мер защиты.

«ДиалогНаука» предлагает полный спектр консалтинговых услуг по разработке, внедрению и сопровождению комплексных систем обеспечения информационной безопасности. Все наши услуги сгруппированы в единый цикл и включают в себя следующие основные этапы:

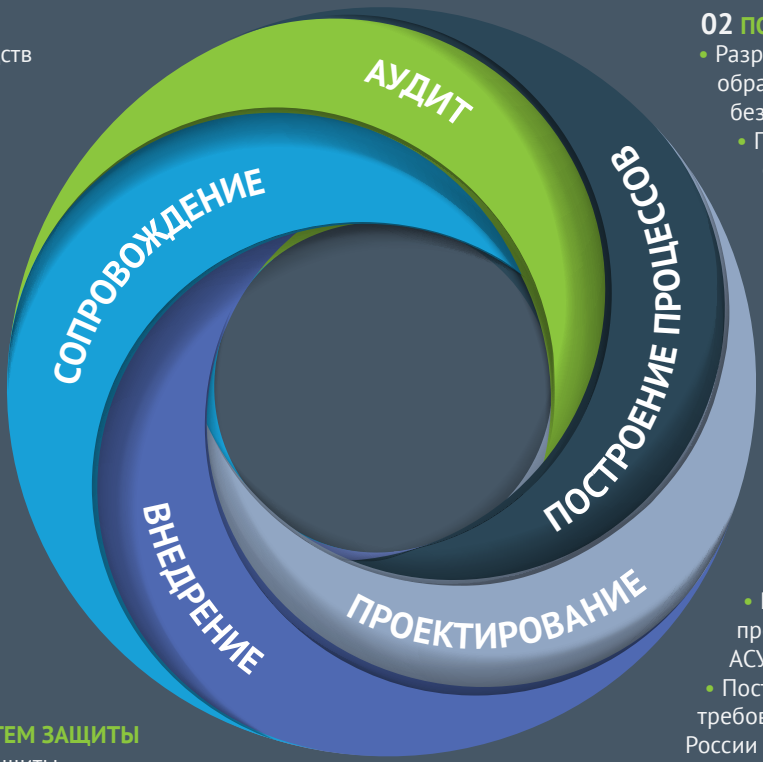
- Проведение аудита информационной безопасности.
- Построение процессов обеспечения информационной безопасности.
- Проектирование комплексной системы обеспечения информационной безопасности.
- Внедрение программных и технических средств защиты информации.
- Техническое сопровождение систем обеспечения информационной безопасности.

01 АУДИТ

- Комплексный аудит ИБ
- Оценка соответствия требованиям ФЗ «О персональных данных»
- Оценка соответствия требованиям стандарта Банка России
- Аудит на соответствие требованиям международного стандарта ISO / IEC 27001
- Аудит на соответствие требованиям стандарта PCI DSS
- Оценка соответствия требованиям ФЗ «О коммерческой тайне»
- Оценка соответствия информационных систем (аттестация, декларирование соответствия)
- Тестирование на проникновение
- Инструментальный аудит ИБ
- Аудит веб-приложений
- Аудит наличия конфиденциальной информации в сети Интернет
- Оценка соответствия требованиям Положения Банка России 382-П
- Аудит и оценка соответствия требованиям Приказа ФСТЭК №31 и стандартов NIST SP800-82, IEC 62443

05 СОПРОВОЖДЕНИЕ

- Техническая поддержка средств защиты информации
- Аутсорсинг технической поддержки и управление средствами и системами ИБ
- Техническое сопровождение центра управления информационной безопасностью (SOC)
- Сопровождение систем защиты персональных данных
- Сопровождение при проверках со стороны регулирующих органов
- Расследование инцидентов информационной безопасности и вирусных заражений
- Обучение по вопросам ИБ
- Сопровождение систем защиты АСУ ТП



02 ПОСТРОЕНИЕ ПРОЦЕССОВ

- Разработка и внедрение процессов обработки и обеспечения безопасности персональных данных
- Построение СОИБ в соответствии с требованиями стандарта Банка России
- Построение СУИБ в соответствии с требованиями стандарта ISO / IEC 27001
- Внедрение процессов обеспечения ИБ данных индустрии платежных карт – PCI DSS
- Построение комплексной системы защиты информации ограниченного доступа, коммерческой тайны
- Разработка системы документации по вопросам обеспечения ИБ
- Разработка и внедрение отдельных процессов обеспечения ИБ (в т.ч. для АСУ ТП)
- Построение СОИБ в соответствии с требованиями Положения Банка России 382-П

04 ВНЕДРЕНИЕ СИСТЕМ ЗАЩИТЫ

- Поставка средств защиты информации
- Макетирование и стендовые испытания средств защиты информации
- Внедрение центров управления информационной безопасностью (SOC)
- Внедрение систем защиты АСУ ТП

03 ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ

- Разработка технических заданий и требований к СЗИ
- Разработка проектной документации на СЗИ
- Разработка рабочей и эксплуатационной документации СЗИ
- Проектирование систем защиты АСУ ТП

ЭТАПЫ

01

Аудит информационной безопасности проводится с целью анализа текущего состояния защищенности компании от внешних и внутренних угроз.

02

Построение и внедрение процессов обеспечения информационной безопасности осуществляется на основе полученной оценки на этапе аудита. Это предполагает разработку политики безопасности и ряда вспомогательных нормативных документов, определяющих требования по защите информации, а также порядок их выполнения и контроля. Внедрение процессов может осуществляться с учетом международных и российских стандартов по защите информации.

Работы выполняются как в комплексе, так и по отдельности, в зависимости от решаемых Заказчиком задач. Такой дифференцированный подход позволяет поэтапно выполнять работы по реализации комплекса организационно-технических мер защиты, давая Заказчику возможность эффективно распределить по времени затраты и временные ресурсы своих сотрудников.

РАБОТ

03

При проектировании комплексной системы защиты информации осуществляется выбор технических решений, средств и мер защиты, которые будут использоваться для обеспечения информационной безопасности.

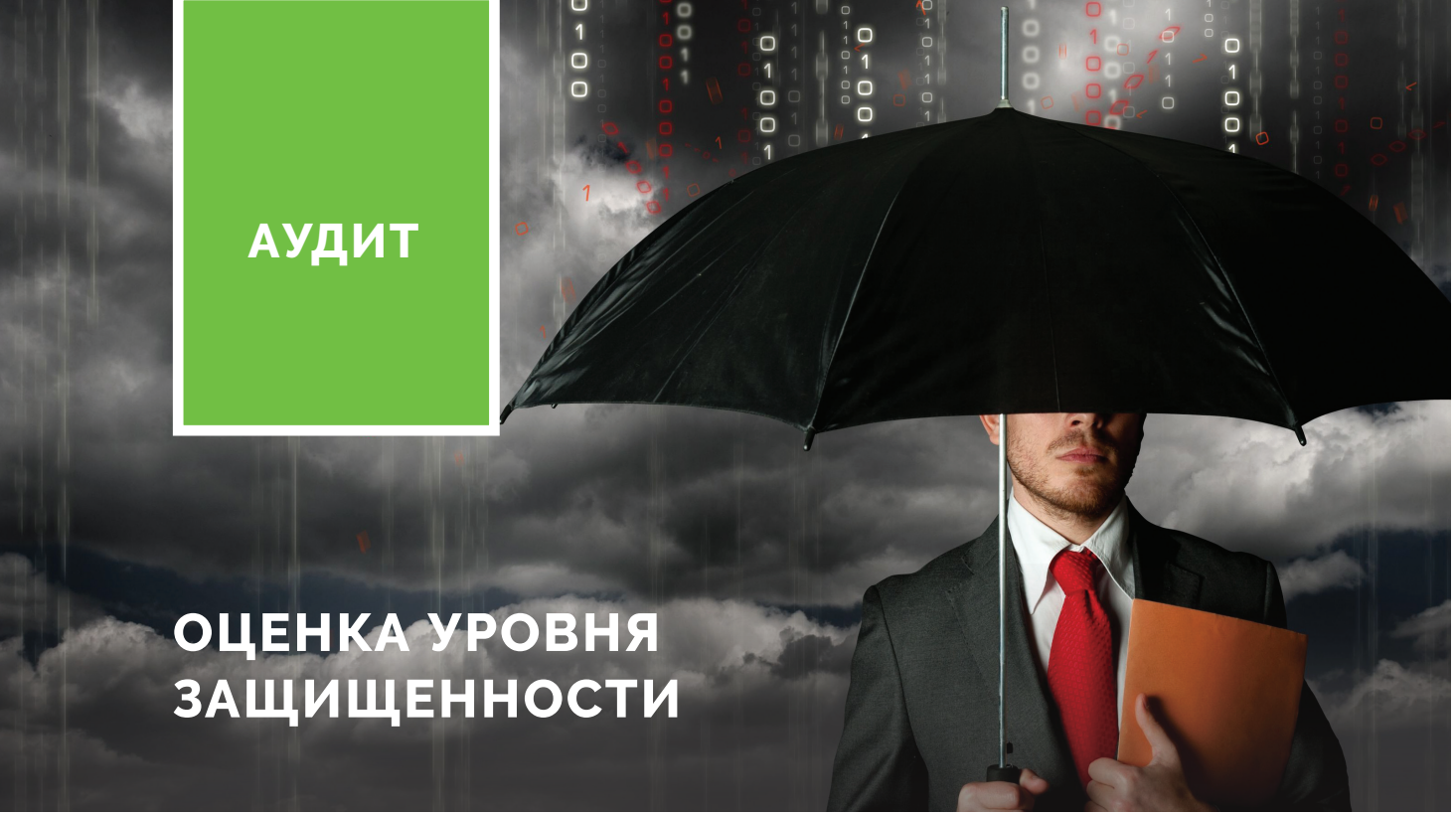
04

При внедрении систем защиты осуществляется установка и конфигурирование средств защиты, опытная эксплуатация, обучение персонала.

05

Сопровождение системы обеспечения информационной безопасности может включать: консультации по базовой установке, штатной работе и обновлению средств защиты; проведение работ по масштабированию или модернизации системы; проведение работ по адаптации под изменения в нормативной документации.

Эксперты нашей компании подберут наиболее удобную форму предоставления услуг и оптимальный состав работ, исходя из индивидуальных особенностей вашей организации, а также из соображений экономической эффективности.



АУДИТ

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ

В зависимости от объекта, защищенность которого требуется оценить, и задач, стоящих перед Заказчиком, наша компания предлагает следующие услуги в области аудита информационной безопасности:

- Инструментальный аудит защищенности.
- Оценка защищенности веб-приложений.
- Анализ исходного кода.
- Тестирование на проникновение.

ИНСТРУМЕНТАЛЬНЫЙ АУДИТ ЗАЩИЩЕННОСТИ

Инструментальный аудит защищенности целесообразно проводить с целью периодического контроля изменений в защищаемой ИТ-инфраструктуре, обнаружения новых уязвимостей, а также проверки фактов устранения ранее выявленных уязвимостей. При проведении данного вида аудита используются одновременно несколько специализированных инструментальных средств. Наша компания предлагает проводить инструментальный аудит защищенности сетевого периметра компании, а также критичных информационных ресурсов на периодической основе.

ОЦЕНКА ЗАЩИЩЕННОСТИ ВЕБ-ПРИЛОЖЕНИЙ

При проведении анализа защищенности веб-приложений используется методика, базирующаяся на методологии и стандартах OWASP (Open Web Application Security Project), STIG (Security Technical Implementation Guide), а также рекомендациях по информационной безопасности разработчиков ПО и средств защиты информации. Как правило, аудит проводится методом Black Box, т. е. без использования аутентификационной или какой-либо другой информации о веб-приложениях. При необходимости возможно проведение анализа защищенности веб-приложений методом Grey Box с использованием непривилегированных учетных записей.

Данные, получаемые в результате такого аудита, обрабатываются экспертами «ДиалогНауки». В процессе обработки происходит оценка возможности эксплуатации выявленных уязвимостей, уровня их критичности, а также возможности их комбинированного использования.

АНАЛИЗ ИСХОДНОГО КОДА

Работы по анализу исходного кода проводятся в тех случаях, когда требуется аудит критичного для бизнеса компании приложения или сервиса с точки зрения выявления уязвимостей. Ручной анализ исходных кодов является крайне трудоемким и обеспечивает хороший результат только при привлечении квалифицированных специалистов. Современные автоматизированные средства анализа защищенности исходного кода позволяют осуществлять такой контроль с минимальными затратами, однако его результаты должны дополнительно интерпретироваться экспертами. Наша компания предлагает использовать комбинированный способ анализа исходного кода, который сочетает в себе преимущества автоматизированного анализа с последующей детализацией и интерпретацией экспертами. В рамках аудита также возможна демонстрация эксплуатации уязвимости и подготовка сигнатур для средств Web Application Firewall.

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Наиболее эффективным инструментом наглядной демонстрации рисков и угроз информационной безопасности является тестирование на проникновение — имитация действий реального злоумышленника по осуществлению вторжения в корпоративную сеть компании и получения доступа к наиболее ценным информационным активам.

Реальному злоумышленнику никогда не поставят задачу произвести поиск уязвимостей целевой информационной системы и анализ критичности обнаруженных уязвимостей для бизнеса. Хакерство — это тот же самый бизнес, суть которого сводится к извлечению прибыли при минимизации рисков и издержек путем причинения вполне определенного ущерба другому бизнесу — бизнесу целевой компании.

При планировании тестирования на проникновение выбирается несколько объектов, получение контроля над которыми может являться целью реального компьютерного преступника. Такими объектами могут быть, например, ноутбук генерального директора (не столько файлы на этом ноутбуке, сколько встроенные в этот ноутбук веб-камера и микрофон), домен Windows локальной вычислительной сети (с целью получения привилегий администратора домена с соответствующими привилегиями на всех включенных в этот домен системах).

Тестирование на проникновение — имитация действий реального компьютерного взломщика — должно осуществляться с максимальным приближением к действительности. Чем ближе к действительности и чем более квалифицированно будет произведена такая работа, тем более ее результаты будут убедительными и очевидными для бизнеса. И тем вероятнее эти результаты приведут к желаемому итогу — повышению осведомленности бизнеса о свойственных ему рисках и угрозах информационной безопасности и созданию у бизнеса финансовой мотивации к решению этой проблемы.

Возможные векторы атак при проведении тестирования на проникновение

Вектор атаки	Описание	Моделируется локально	Моделируется удаленно
Физический	Атаки с использованием непосредственного физического доступа внутрь защищаемого периметра корпоративной сети (если таковой есть)	✓	
Сетевой	Удаленные атаки на сетевые ресурсы и протоколы		✓
Электронная почта	Атаки с использованием электронной почты (в том числе с элементами социальной инженерии)		✓
Приложения	Атаки с использованием специфических приложений, используемых Заказчиком (например, интернет-портал)		✓
Беспроводные сети	Атаки, направленные на беспроводные протоколы передачи данных 802.11 (Wi-Fi), 802.15 (Bluetooth), 802.16 (Wi-Max)	✓	
Клиентские приложения	Атаки на клиентские приложения		✓
Мобильные устройства	Атаки на мобильные устройства (мобильные и переносные компьютеры, смартфоны и т. д.)	✓	
Социальная инженерия	Атаки на пользователей с использованием методов социальной инженерии	✓	✓

При проведении любого из описанных выше типов оценки уровня защищенности, специалисты нашей компании подготовят отчет, содержащий детальное описание всех выявленных уязвимостей, возможных способов их эксплуатации, а также рекомендации по их устранению. Дополнительно также может разрабатываться презентация по результатам аудита для руководства Организации.

КОМПЛЕКСНЫЙ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит информационной безопасности — это комплекс работ, позволяющих провести независимую экспертную оценку текущего состояния (уровня зрелости) процессов управления и обеспечения информационной безопасности организации и определить степень её соответствия критериям аудита.

Основные задачи, решаемые при проведении аудита информационной безопасности:

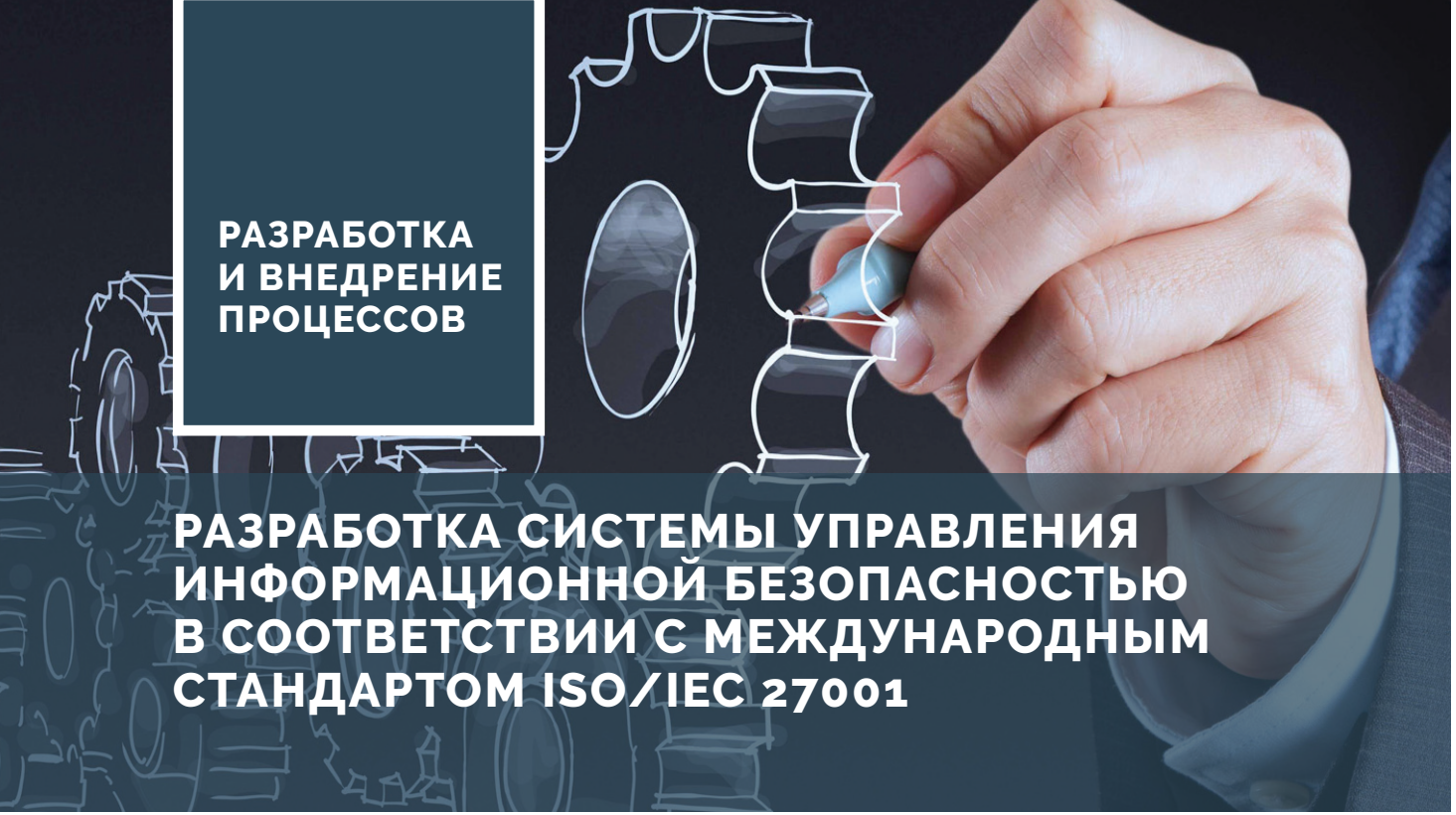
- определение адекватных мер по обеспечению информационной безопасности, соответствующих бизнес-целям организации, требованиям регуляторов, российских и международных стандартов по информационной безопасности;
- определение приоритетных направлений развития системы обеспечения информационной безопасности, нацеленных на повышение устойчивости функционирования организации и эффективность ведения бизнеса за счет максимального снижения информационных рисков и финансовых потерь, связанных с угрозами информационной безопасности.

Варианты аудита информационной безопасности, предлагаемые «ДиалогНаукой», зависят от критериев аудита, выбранных Заказчиком, и могут включать как по отдельности, так и в комплексе следующие работы:

- оценка уровня защищенности систем и приложений организации;
- тестирование на устойчивость к атакам класса «отказ в обслуживании» как на логическом (уровень приложений), так и на сетевом уровне по отношению к ценным информационным активам;
- оценка соответствия требованиям законодательства Российской Федерации (в том числе Федерального закона «О персональных данных»);
- оценка соответствия требованиям стандарта ISO / IEC 27001;
- оценка соответствия требованиям PCI DSS;
- оценка соответствия требованиям СТО БР ИББС и Положения Банка России 382-П;
- аудит наличия конфиденциальной информации в сети Интернет;
- комплексный аудит информационной безопасности, включающий в себя реализацию нескольких направлений работ, в том числе при желании Заказчика проведение оценки рисков информационной безопасности.

По результатам аудита информационной безопасности разрабатывается отчет, как правило, содержащий:

- описание технологических и организационных процессов обеспечения информационной безопасности;
- результаты оценки (анализа) существующих процессов обеспечения информационной безопасности;
- результаты инструментального анализа защищенности корпоративной информационной системы;
- рекомендации по устранению выявленных недостатков в процессах обеспечения информационной безопасности;
- рекомендации по устранению выявленных эксплуатационных уязвимостей;
- рекомендации по внедрению новых процессов обеспечения информационной безопасности;
- рекомендации по разработке новых и внесению изменений в существующие документы, регламентирующие вопросы обеспечения информационной безопасности;
- рекомендации по внедрению дополнительных механизмов (средств) обеспечения информационной безопасности.



РАЗРАБОТКА И ВНЕДРЕНИЕ ПРОЦЕССОВ

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СООТВЕТСТВИИ С МЕЖДУНАРОДНЫМ СТАНДАРТОМ ISO/IEC 27001

Применение риск-ориентированного подхода к построению системы управления информационной безопасностью (далее — СУИБ) на базе общепризнанного международного стандарта ISO/IEC 27001 позволяет создать интегрированную в общую систему управления организации инфраструктуру безопасности, учитывающую бизнес-требования и цели организации.

Стандарт устанавливает требования к «контролям» безопасности (контроль — процесс, обеспечивающий достижение системой поставленных целей), подлежащим внедрению в соответствии с индивидуальными потребностями организации.

«ДиалогНаука» является официальным партнером BSI Management Systems и оказывает услуги по разработке и внедрению СУИБ.

Каждая организация может преследовать разные цели при внедрении СУИБ, например:

- создание внутреннего инструмента для эффективного управления информационной безопасностью и принятия тактических и/или стратегических решений;
- создание конкурентных преимуществ товара и/или услуг организации с точки зрения информационной безопасности (маркетинг);
- демонстрация деловым партнерам приверженности принципам информационной безопасности;
- необходимость соблюдения требований контрактов и условий тендеров (требования клиентов / заказчиков / партнеров по защите информации).

В соответствии со стандартом ISO / IEC 27001 СУИБ должна проектироваться таким образом, чтобы обеспечить выбор адекватных и соразмерных мер по обеспечению информационной безопасности. Меры должны быть направлены на поддержание определенных владельцами информационных активов свойств безопасности (конфиденциальности, целостности и/или доступности) и обеспечение заданного «целевого» уровня информационной безопасности.

Для определения текущего уровня зрелости процессов в рамках СУИБ организации может проводиться аудит информационной безопасности (предпроектное обследование уровня информационной безопасности).

Все работы по созданию и внедрению СУИБ можно разбить на следующие основные этапы:

- определение области действия СУИБ;
- проведение обследования с целью идентификации и классификации информационных активов, входящих в область действия СУИБ;
- проведение оценки и анализа рисков информационной безопасности;
- разработка политики информационной безопасности организации;
- определение защитных мер контроля и их обоснование для минимизации рисков (выбор средств контроля);
- разработка нормативно-методических документов, формализующих процессы обеспечения информационной безопасности в рамках СУИБ;
- внедрение процессов СУИБ;
- проведение контрольного аудита информационной безопасности на соответствие требованиям ISO / IEC 27001;
- подготовка к сертификации СУИБ компании на соответствие требованиям стандарта ISO 27001.

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ МЕЖДУНАРОДНОГО СТАНДАРТА PCI DSS

Требования стандарта PCI DSS распространяются на банки, торгово-сервисные предприятия, поставщиков технологических услуг и другие организации, деятельность которых связана с обработкой, передачей и хранением данных о держателях платежных карт, т. е. организации, работающие с международными платёжными системами VISA, MasterCard, American Express, JCB и Discover.

Любая Компания, обрабатывающая, хранящая или передающая в течение года информацию хотя бы об одной карточной транзакции или владельце платежной карты, должна соответствовать требованиям стандарта PCI DSS.

Международные платежные системы обязывают Компании, на которые распространяются требования стандарта, проходить регулярную проверку соответствия этим требованиям: ежегодные аудиторские проверки, ежеквартальные сканирования сетей и в некоторых случаях заполнение листа самооценки (Self-Assessment Questionnaires, SAQ).

Для выполнения аудита Компании должны привлекать стороннюю организацию, имеющую статус Qualified Security Assessor (QSA).

«ДиалогНаука» обладает необходимым статусом QSA и оказывает полный комплекс услуг по проведению QSA аудита, а также по внедрению требований соответствующих платежных систем и PCI DSS, что позволяет значительно сократить финансовые и ресурсные затраты на создание системы защиты данных о держателях платёжных карт.

«ДиалогНаука» также имеет аккредитацию Approved Scanning Vendor (ASV), которая позволяет проводить ASV сканирования уязвимостей в соответствии с требованиями стандарта PCI DSS.

Комплексный проект по приведению Компании в соответствие требованиям PCI DSS состоит из следующих основных этапов:

1. Обследование и анализ соответствия требованиям международного стандарта PCI DSS, в том числе определение / уточнение области применимости PCI DSS.
2. Внедрение требований стандарта: внедрение процессов обеспечения безопасности данных о держателях платежных карт и системы защиты (технических средств обеспечения безопасности данных о держателях платежных карт).
3. Проведение тестирования на проникновение и ASV сканирования.
4. Выполнение самооценки или проведение сертификационного QSA аудита.

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ СТАНДАРТА БАНКА РОССИИ И ФЕДЕРАЛЬНОГО ЗАКОНА «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»

Комплекс документов БР ИББС — это взаимоувязанная совокупность документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

Построение системы информационной безопасности в кредитной организации в соответствии с Комплексом документов БР ИББС предоставляет следующие преимущества:

- соответствие отраслевому стандарту;
- повышение стабильности функционирования системы обеспечения информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности за счет применения взаимосвязанного комплекса превентивных мер и процессов реагирования на инциденты;
- повышение доверия к банку;
- минимизация рисков информационной безопасности как части операционных рисков;
- поддержка информированности руководства организации об информационной безопасности;
- разделение полномочий и ответственности за контроль и выполнение процессов обеспечения информационной безопасности;
- обеспечение адекватной защиты информации, отнесенной к персональным данным, банковской и коммерческой тайне.

Наряду с требованиями Комплекса БР ИББС кредитные организации должны выполнять требования, установленные Федеральным законом «О национальной платежной системе» и Положением Банка России от 9.06.2012 № 382-П (далее — Положение 382-П).

Данное Положение 382-П распространяется и на других субъектов в рамках национальной платежной системы: операторов платежных систем, банковских платежных агентов (субагентов), операторов инфраструктуры и т. д.

Требования Положения 382-П на 80 % соответствуют основным требованиям Комплекса БР ИББС в части требований к системе информационной безопасности, а также основным процессам системы менеджмента информационной безопасности.

Все субъекты платежных систем должны не реже одного раза в два года проводить оценку выполнения установленных Положением 382-П требований. Такая оценка может проводиться либо в форме самооценки, либо с привлечением внешнего аудитора, обладающего лицензией ФСТЭК на ТЗКИ, в соответствии с требованиями Постановления Правительства РФ от 13.06.2012 № 584

Работы по построению системы обеспечения информационной безопасности в соответствии с требованиями Положения 382-П и/или Комплекса БР ИББС состоят из следующих основных этапов:

1 Предварительная оценка уровня информационной безопасности и выявление несоответствий (GAP анализ), по результатам которой формируется и согласовывается с заказчиком перечень мер по устранению выявленных недостатков.

2 Определение достаточности имеющихся средств защиты информации и при необходимости разработка рекомендаций по дополнительным средствам, включая формирование требований к комплексу технических мер обеспечения информационной безопасности, состоящему из имеющихся и дополнительных средств защиты. При необходимости может выполняться разработка технического задания на проектирование и внедрение комплекса средств защиты информации.

3 Доработка (разработка) необходимых документов, формализующих процессы обеспечения информационной безопасности.

4 После утверждения всех разработанных/доработанных документов и внедрения процессов (в том числе получение адекватных свидетельств выполнения процессов управления и обеспечения информационной безопасности) проводится заключительная оценка соответствия требованиям Положения 382-П и/или комплекса БР ИББС.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СИСТЕМ

ВНЕДРЕНИЕ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Каждая организация по мере своего развития и роста обязательно проходит этап, когда нужно построить целый ряд процессов, таких как управление IT-инфраструктурой и обеспечение информационной безопасности. Эти задачи могут возникнуть как вследствие необходимости выполнения требований законодательства и отраслевых требований, так и вследствие потребности бизнеса в более эффективном управлении.

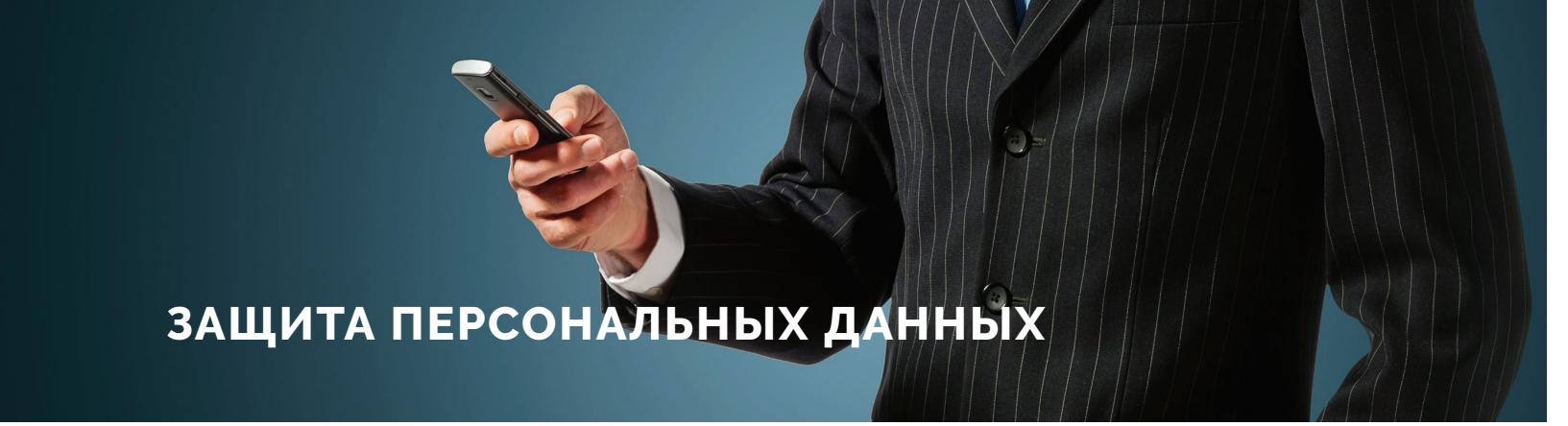
«ДиалогНаука» имеет обширный опыт построения комплексных систем обеспечения информационной безопасности, что позволяет реализовывать проекты любой сложности. При реализации того или иного процесса обеспечения информационной безопасности, в зависимости от уровня зрелости существующих процессов, осуществляется разработка необходимого набора документации, техническое проектирование и внедрение системы защиты, а также ее дальнейшая поддержка. Наиболее критичным является формирование оптимальных направлений технического и технологического развития процессов обеспечения информационной безопасности с учетом отраслевой специфики, уже достигнутого уровня зрелости и существующих процессов управления.

Для успешного и эффективного внедрения процессов обеспечения информационной безопасности «ДиалогНаука» принимает во внимание как факторы информационной безопасности, так и факторы, непосредственно связанные с развитием и использованием информационных технологий, а также бизнес-факторы, рассматривая совокупность технологических и бизнес-процессов, поскольку многие из них являются в значительной степени интегрированными между собой.

В качестве примеров процессов обеспечения информационной безопасности можно привести следующие:

- процесс управления информационными активами;
- процесс управления рисками информационной безопасности;
- процесс управления документацией в области информационной безопасности;
- процесс управления записями в области информационной безопасности;
- процесс мониторинга и анализа системы управления информационной безопасностью;
- процесс анализа системы управления информационной безопасностью со стороны руководства;
- процесс аудита информационной безопасности;
- процесс назначения и распределения ролей в области информационной безопасности;
- процесс антивирусной защиты;
- процесс использования ресурсов сети Интернет;
- процесс криптографической защиты информационных активов;
- процессы аудита и мониторинга информационной безопасности;
- процесс обеспечения физической безопасности;
- процесс управления и контроля доступа;
- процесс обеспечения информационной безопасности на стадиях жизненного цикла информационных систем;
- процессы обеспечения непрерывности деятельности;
- процессы управления инцидентами информационной безопасности и др.

При реализации проекта по защите информации организация может выбрать только те процессы, которые необходимо формализовать и внедрить. В ходе выполнения работ консультантами «ДиалогНаука» оказывается методическая помощь, связанная с первичным внедрением данных процессов в организации.



ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В настоящее время проблема защиты персональных данных по-прежнему является одной из наиболее актуальных для многих российских компаний. Это обусловлено и участившимися жалобами со стороны субъектов персональных данных, и увеличением числа проверок и обращений со стороны органов надзора, и, конечно, периодическими изменениями в требованиях нормативных документов, влекущими усложнение процедур построения систем защиты персональных данных.

Для создания и внедрения системы защиты персональных данных предлагаем комплекс услуг, который включает в себя следующие работы:

- проведение обследования процессов обработки и защиты персональных данных, формирование рекомендаций по устранению выявленных несоответствий требованиям ФЗ «О персональных данных»;
- разработка модели нарушителя и угроз безопасности персональных данных с последующим определением требуемого уровня защищенности персональных данных;
- проектирование системы защиты в составе информационной системы, обрабатывающей персональные данные;
- разработка пакета организационно-распорядительной документации по вопросам обработки и защиты персональных данных;
- внедрение системы защиты персональных данных;
- оценка соответствия информационной системы персональных данных.

Процедура обследования информационных систем персональных данных (ИСПДн) необходима для:

- определения перечня обрабатываемых персональных данных и легальности их обработки;
- определения перечня и состава ИСПДн, в том числе для последующего формирования требований к защите ПДн;
- описания взаимодействия Компании с другими Операторами и субъектами ПДн.

На основе информации, собранной в процессе обследования, разрабатывается модель нарушителя и угроз безопасности ПДн и осуществляется определение требуемого уровня защищенности ПДн.

Уровень защищенности персональных данных определяется в соответствии с требованиями Постановления Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в ИСПДн» в зависимости от типов актуальных угроз безопасности, определенных при моделировании, объема и состава обрабатываемых персональных данных.

В рамках проектирования системы защиты ПДн осуществляется разработка технического задания, макетирование и стендовые испытания средств защиты информации, разработка документов технического проекта. В процессе проектирования также разрабатывается пакет эксплуатационной и организационно-распорядительной документации, регламентирующей порядок обработки и обеспечения безопасности ПДн в Компании. Данные работы проводятся в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн» с учетом особенностей ИТ-инфраструктуры информационных систем Компании и применяемых в Компании средств защиты.

Следующий шаг — внедрение системы защиты персональных данных, в ходе которого осуществляется поставка, установка и настройка всего комплекса средств защиты информации, определенного при проектировании. При необходимости на данном этапе может проводиться обучение персонала правилам работы со средствами защиты, а также разработка дополнительных инструкций, руководств и иных эксплуатационных документов.

Завершающий этап работ — оценка соответствия информационной системы, обрабатывающей ПДн, требованиям законодательных и нормативных документов. Необходимость проведения такой оценки обусловлена положениями Постановления Правительства Российской Федерации № 1119 и требованиями Приказа ФСТЭК России от 18.02.2013 № 21.

По выбору Оператора ПДн оценка может быть проведена как в форме самооценки (декларации), так и в форме аттестации информационной системы на соответствие требованиям по безопасности.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

«ДиалогНаука» предлагает услуги по проектированию и внедрению комплексных систем обеспечения информационной безопасности.

В качестве объекта защиты может выступать как вся система в целом, так и отдельные её подсистемы и компоненты, такие как:

- корпоративная локальная вычислительная сеть, сеть филиала и т. д.;
- интернет-сервисы компании: системы ДБО, корпоративные облачные сервисы, сайт компании и др.;
- критичные информационные системы: ERP, CRM, система электронной почты и др.

Услуга предполагает выполнение цикла работ, состоящего из следующих основных этапов:

1 Предпроектное обследование. Этот этап включает в себя обследование объекта защиты Заказчика с целью сбора и анализа исходных данных, необходимых для проектирования комплексной системы защиты. Сбор данных осуществляется путём интервьюирования сотрудников Заказчика, анализа существующей технической документации, а также с помощью специализированных инструментальных средств.

2 Формирование требований. На этом этапе осуществляется разработка технического задания на создание (модернизацию) комплексной системы защиты и его утверждение у Заказчика. Техническое задание разрабатывается специалистами компании «ДиалогНаука» и содержит требования к создаваемой системе, сформированные с учетом целей и задач системы, особенностей объекта защиты, пожеланий Заказчика, наличия у него персонала и его квалификации, требований надежности, совместимости, минимизации затрат на внедрение и эксплуатацию и др.

3 Техническое проектирование комплексной системы защиты заключается в разработке проектных решений по обеспечению информационной безопасности, а также рабочей и эксплуатационной документации на проектируемый комплекс защиты.

Комплексные проектные решения могут включать в себя:

- защиту от угроз «нулевого дня» и целенаправленных атак APT (Advanced Persistent Threat);
- мониторинг событий информационной безопасности;
- организацию защищенного информационного взаимодействия на базе сетей VPN;
- защиту от утечки конфиденциальной информации (DLP);
- контроль интернет-трафика;
- организацию защищённого доступа к сети Интернет;
- контроль действий администраторов системы и привилегированных пользователей;
- выявление уязвимостей программного обеспечения системы;
- контроль защищенности информационных ресурсов;
- управление мобильными устройствами (MDM);
- выявление и предотвращение сетевых атак (IDS / IPS);
- защиту от вредоносного кода и спама и т. д.

Проектные решения могут базироваться как на основе уже существующих коммерческих средств защиты, так и на специализированных решениях, разработанных или адаптированных под нужды Заказчика.

4 Ввод в действие комплексной системы обеспечения информационной безопасности. На этом этапе осуществляется установка и настройка системы защиты на объектах Заказчика, проведение опытной эксплуатации, приемочные испытания.

5 Обучение по вопросам эксплуатации комплексной системы защиты проводится для администраторов безопасности, системных администраторов, пользователей системы. Высококвалифицированные инженеры и консультанты, обладающие многолетним практическим опытом работы в области информационной безопасности, проводят обучение в форме семинаров. Практические занятия проводятся на стендах, включающих в себя рабочие станции и серверы, а также средства защиты информации, и позволяют моделировать фрагменты комплексной системы защиты и окружения, в котором она функционирует у Заказчика. Обучение с использованием таких стендов позволяет на практике отрабатывать сценарии использования компонентов комплексной системы защиты.

Конкретный состав работ по каждому этапу формируется на основе характеристик существующей автоматизированной системы Заказчика, а также состава проектируемой системы обеспечения информационной безопасности.

СОПРОВОЖДЕНИЕ СРЕДСТВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Современные средства и системы информационной безопасности характеризуются следующими особенностями:

- Глубокая интеграция в ИТ-инфраструктуру предприятия средств защиты информации — внесение незначительных изменений в настройки системы влияет на эффективность работы как отдельных средств защиты, так и всей системы защиты, а отказы в работе СЗИ могут негативно отражаться на работе предприятия в целом.
- Наличие большого количества функций СЗИ, сложность пользовательских интерфейсов и взаимозависимость параметров настроек СЗИ обуславливают высокие требования к квалификации обслуживающего персонала.
- Наличие у современных СЗИ функций по автоматическому информированию персонала, функций по анализу событий безопасности и функций по формированию отчетности о состоянии информационной безопасности защищаемых ИС обуславливает потребность в «тонких» комплексных настройках СЗИ, возможных только на работающей защищаемой ИС.
- Необходимость реализации политик ИБ, вытекающих из нормативной документации, с помощью СЗИ, организации постоянного контроля показателей информационной безопасности и принятия корректирующих мер требуют наличия у Заказчика налаженных процессов ИБ.

Указанные особенности формируют необходимость привлечения для эксплуатации СЗИ опытных, квалифицированных специалистов по СЗИ, операторов СЗИ, а также сотрудников, обеспечивающих поддержку пользователей, что существенно увеличивает стоимость владения средствами защиты.

«ДиалогНаука» предлагает следующие наборы услуг, облегчающие Заказчику эксплуатацию СЗИ:

- **Информационное сопровождение**

  Позволит Заказчику поддерживать в актуальном состоянии документацию на систему обеспечения безопасности, поддерживать необходимый уровень осведомленности сотрудников и быть своевременно проинформированным об изменениях нормативных документов и сопровождении регуляторами. Эти услуги являются востребованными, в частности, для информационного обеспечения систем защиты персональных данных.

- **Техническое сопровождение**

  Направлено на оказание содействия Заказчику при возникновении технических проблем, возникающих в процессе эксплуатации СЗИ, обеспечения непрерывности работы СЗИ и помощи в контроле уровня защищенности.

- **Сервисное сопровождение**

  Позволит передать значительную часть задач, связанных с сопровождением СЗИ, на аутсорсинг. Это поможет минимизировать риски информационной безопасности, при этом не увеличивая расходов, за счет повышения эффективности работы СЗИ и организации процессов обеспечения информационной безопасности.

Состав оказываемых услуг представлен в таблице:

Тип услуги	Информационное сопровождение	Техническое сопровождение	Сервисное сопровождение
Услуга по технической поддержке СЗИ			
Консультации по работе СЗИ		✓	✓
Удаленная техническая поддержка		✓	✓
Аварийные выезды		✓	✓
Ремонт и замена вышедших из строя компонентов аппаратного обеспечения		✓	✓
Услуга по обеспечению непрерывности работы СЗИ			
Предоставление проверенных обновлений ПО		✓	✓
Установка согласованных обновлений ПО			✓
Регламентные работы с использованием удаленного подключения		✓	✓
Профилактические выезды		✓	✓
Управление СЗИ			✓
Услуга по сопровождению модернизации ИС			
Сопровождение модернизации ИС (реализация изменений)			✓
Сопровождение ОРД	✓		✓
Разработка новых ОРД	✓		✓

Тип услуги	Информационное сопровождение	Техническое сопровождение	Сервисное сопровождение
Услуга по контролю уровня защищенности			
Ежедневный анализ событий в консоли управления			✓
Ежемесячный анализ зарегистрированных событий			✓
Анализ защищенности сетевого периметра		✓	✓
Подключение к системе мониторинга событий ИБ (SIEM)			✓
Квартальные рекомендации по совершенствованию			✓
Услуга по повышению осведомленности работников в вопросах ИБ			
Технические семинары для администраторов/ операторов СЗИ	✓		✓
Повышение осведомленности персонала по вопросам ИБ	✓		✓
Услуга по сопровождению мер по выполнению требований законодательства по ИБ			
Поддержка аттестации ИС (ИСПДн)	✓		✓
Поддержка Компании при проведении проверок контролирующими органами	✓		✓
Услуга по информационной поддержке Компании			
Информационная поддержка СОИБ (СЗПДн)	✓		✓
Уведомление о выходе обновлений ПО СЗИ		✓	✓
Предоставление отчетов о результатах оказания услуг		✓	✓

КОНТАКТНАЯ ИНФОРМАЦИЯ:

117105, Москва, ул. Нагатинская, 1

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

Email: info@dialognauka.ru
Website: www.dialognauka.ru