ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

✓ Эффективная ✓ Сбалансированная ✓ Экономически оправданная

УСЛУГИ

- Аудит информационной безопасности
- Тестирование на проникновение
- Разработка организационно-распорядительной документации
- Управление рисками информационной безопасности
- Обеспечение непрерывности бизнеса
- Обеспечение соответствия требованиям Федерального закона РФ № 152-ФЗ «О персональных данных» Обеспечение соответствия требованиям Федерального закона РФ № 161-ФЗ «О национальной платежной системе»
- Обеспечение соответствия требованиям СТО БР ИББС
- Обеспечение соответствия требованиям ISO 27001/ГОСТ Р ИСО/МЭК 27001-2006
- Обеспечение соответствия требованиям Федерального закона РФ № 187-ФЗ «О безопасности КИИ РФ» Услуги по построению комплексных систем защиты информации (СЗИ)


Консалтинг


Аудит


Проектирование


Внедрение


Аттестация


Сопровождение

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Управление информационной безопасностью

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Комплексный анализ системы защиты информации компании позволяет выявить объективную картину ее текущего состояния.
В результате независимой всесторонней оценки заказчик получает возможность:

- установить слабые и потенциально уязвимые места системы ИБ, вероятные риски;
- сформировать детальный план по улучшению системы ИБ, включающий в себя проект бюджета и организационно-штатные мероприятия.

По итогам проведения аудита заказчику предоставляется пакет документов, который содержит подробный отчет, план мероприятий по совершенствованию/доработке системы ИБ, модели угроз и потенциального нарушителя.

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Тест на проникновение (penetration-test) – это возможность взглянуть на корпоративную систему защиты информации глазами злоумышленника и получить представление о реальной степени защищенности информационных активов.
Тест проводится всеми средствами и приемами, которые используют злоумышленники (внутренние/внешние).

На основе результатов теста на проникновение можно:

- продемонстрировать вероятные сценарии и результаты успешной атаки злоумышленников на ресурсы компании;
- получить актуальную независимую оценку состояния системы ИБ;
- определить необходимые мероприятия для повышения уровня ИБ.

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Управление информационной безопасностью

РАЗРАБОТКА ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ

Комплекс организационно-распорядительной документации (ОРД) устанавливает требования, предъявляемые к информационной безопасности в компании. Разработка и внедрение ОРД необходимы для нормального функционирования системы защиты информации, для единого понимания корпоративной стратегии развития ИБ всеми сотрудниками компании.

Как правило, комплекс документации подразделяют на 3 уровня:

- концепция, политика ИБ;
- регламенты, правила, частные политики обеспечения ИБ;
- инструкции администраторов, различные журналы учета.

При разработке документов учитываются как отечественные стандарты и рекомендации, так и мировые **– ISO, NIST** и др

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для организаций с крупной или быстро развивающейся информационной инфраструктурой базового уровня информационной безопасности может оказаться недостаточно.
Мы рекомендуем провести анализ рисков, который позволит получить убедительные обоснования для принятия управленческих решений по совершенствованию ИБ. Управление рисками представляет собой процесс, направленный на уменьшение уровня рисков и доведение его до приемлемого значения.

После проведения анализа рисков применяется один из следующих подходов:

- принятие риска;
- ликвидация риска посредством устранения причин и/или последствий риска;
- минимизация риска, которая может быть проведена путем уменьшения возможности реализации угрозы или путем уменьшения величины ущерба от ее реализации;
- передача риска, которая осуществляется с помощью других, альтернативных мер компенсации потерь, таких как страхование или заключение с поставщиком договора на обслуживание.

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Управление информационной безопасностью

ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕСА

Система обеспечения непрерывности деятельности компании представляет собой комплекс мер, гарантирующих устойчивую работу организации в чрезвычайных ситуациях, в том числе защиту объектов и персонала, а также стабильность протекания важнейших бизнес-процессов. Построение данной системы осуществляется на основе различных нормативов:

- британский стандарт BS 25999;
- международный стандарт ISO 22301;
- указание ЦБ РФ № 2194-У «О внесении изменений в Положение Банка России от 16 декабря 2003 года»;
- приказ № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»;
- СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;
- ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса»

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Приведение в соответствие (Compliance)

ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ФЕДЕРАЛЬНОГО ЗАКОНА РФ № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Вопросы защиты персональных данных, а также услуги по приведению систем защиты информации в соответствие требованиям законодательства в этой области сегодня актуальны для многих организаций, независимо от их форм собственности и размеров.

Внедрение комплекса мер по защите персональных данных позволяет:

- организовать порядок обработки и защиты информации;
- обеспечить соблюдение строгого соответствия указанных процессов нормативно-правовым требованиям.

Постпроектное сопровождение может включать консалтинговые услуги, периодические проверки порядка обработки и защиты персональных данных.

ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ISO 27001/ГОСТ Р ИСО/МЭК 27001-2006

Стандарт **ISO/IEC 27001:2013** «Information technology – Security techniques – Information security management systems – Requirements» и его российский аналог **ГОСТ Р ИСО/МЭК 27001-2006** «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» подготовлены в качестве модели для разработки, внедрения, функционирования, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ).

Внедрение СМИБ является для компании стратегическим решением.

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Приведение в соответствие (Compliance)

ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ФЗ РФ № 161-ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»

Закон предписывает операторам по переводу денежных средств, банковским платежным агентам (субагентам), операторам платежных систем и услуг платежной инфраструктуры обеспечивать защиту не только персональных данных, но и информации о средствах и методах, применяемых для их защиты, а также иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

Соответствующие требования устанавливают следующие основные нормативные акты:

- **Положение Банка России от 4 июня 2020 г. № 719-П** «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению; защиты информации при осуществлении переводов денежных средств»;
- **Положение Банка России от 9 января 2019 г. № 672-П** «О требованиях к защите информации в платежной системе Банка России»;

Положение № 719-П устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры и банковские платежные агенты (субагенты) обеспечивают защиту информации при осуществлении переводов денежных средств.

Требования **Положения № 672-П** к защите информации в платежной системе Банка России должны выполнять участники платежной системы Банка России, являющиеся кредитными организациями (их филиалами), имеющие доступ к услугам по переводу денежных средств с использованием распоряжений в электронном виде, а также операционный центр, платежный клиринговый центр другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей (далее - участники обмена). Требования распространяются на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, применяемые для обработки защищаемой информации, перечисленной в **пункте 2.1 Положения Банка России от 4 июня 2022 года № 719-П.**

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Приведение в соответствие (Compliance)

ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТО БР ИББС

Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС) – комплекс документов, описывающий единый подход к построению системы защиты информации в организациях банковской сферы с учетом лучших мировых практик менеджмента ИБ, требований российского законодательства, а также отраслевой специфики организаций банковской сферы.

Обеспечение соответствия осуществляется на основе выполнения не только требований системы СТО БР ИБСС, но и следующих нормативов:

- Положение **Банка России от 17 апреля 2019 г. N 683-П** «Об установлении обязательных для кредитных организаций требований к
- обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»;
- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый
- состав организационных и технических мер»;
- **ГОСТ Р 57580.2-2018** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»
- Положение № 683-П устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента.

Требования применяются для обеспечения защиты информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств. **ГОСТ Р 57580.1-2017** определяет уровни защиты информации и соответствующие им требования к содержанию базового состава мер защиты информации, которые применяются финансовыми организациями для реализации требований к обеспечению защиты информации, установленных нормативными актами Банка России. **ГОСТ Р 57580.2-2018** устанавливает требования к методике и оформлению результатов оценки соответствия ЗИ финансовой организации при выборе и реализации организационных и технических мер ЗИ в соответствии с требованиями **ГОСТ Р 57580.1**, применяемых финансовой организацией для реализации требований к обеспечению ЗИ, установленных нормативными актами Банка России.

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Приведение в соответствие (Compliance)

ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ФЕДЕРАЛЬНОГО ЗАКОНА РФ №187-ФЗ «О БЕЗОПАСНОСТИ КИИ РФ»

Федеральный закон **«О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ** регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.
Работы по приведению КИИ Заказчиков в соответствие требованиям 187-ФЗ, а также подзаконным актам включают:

- обследование объектов информатизации и оказание консультативных услуг по категорированию объектов КИИ (**Постановление Правительства РФ №127 от 08.02.2018**), подготовку документации для направления в регулирующие органы;
- формирование требований к системе защиты информации значимых объектов КИИ (**Приказы ФСТЭК России №235 от 21.12.2017, №239 от 25.12.2017 и др**.) с учетом их категории, разработку технического задания; ų разработку технического проекта, рабочей и эксплуатационной документации; ų внедрение средств согласно разработанного технического проекта;
- обеспечения взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) согласно **Приказов ФСБ России №282 от 19 июня 2019 г., № 368 от 24 июля 2018** г. и др

Состав работ может меняться в зависимости от потребностей компании, проводимых в ней ранее мероприятий по защите информации. Вся разрабатываемая документация соответствует требованиям законов, нормативных актов, руководящих документов, ГОСТ, СНиП, ЕСКД, ЕСПД

ГРУППА КОМПАНИЙ Navigator

+7 (812) 495-63-39
+7 (495) 988-64-74
order@nav-it.ru

Комплексные системы защиты

Содержание работ полностью соответствует общепринятым подходам, лучшим практикам, а также рекомендациям и требованиям отечественных и международных стандартов. Как правило, работы выполняются поэтапно и включают в себя:

Предпроектное обследование/аудит

Формирование требований

Эскизное проектирование комплексной системы обеспечения ИБ

Стендовые испытания предварительных проектных решений

Технорабочее проектирование комплексной системы обеспечения ИБ

Внедрение

Опытная эксплуатация

Оценка соответствия (аттестация)

Сопровождение