420087, Республика Татарстан,
г. Казань, ул. Даурская, 41
117545, Москва, Варшавское шоссе,
д. 129а, корп. 2
тел./факс: +7 (843) 5620630
эл. почта: info@onlinesec.ru
веб-сайт: онлайнзащита.рф

41, Daurskaya St., Kazan,
Republic of Tatarstan, Russia, 420087
129a build. 2, Varshavskoe highway
Moscow, Russia, 117545
phone/fax: +7 (843) 5620630
e-mail: info@onlinesec.ru
web: www.onlinesec.ru

Услуги в области Информационной Безопасности

Развитие мирового сообщества наглядно демонстрирует, что в последнее время критически важным ресурсом любой организационной структуры, является информация, циркулирующая в автоматизированных информационных системах этих организаций. Данные системы являются неотъемлемым компонентом структуры управления экономикой, финансами и развитием организации. Ускоренное развитие компьютерных технологий не только в значительной мере способствовало повышению эффективности их функционирования, но и открыло дополнительные возможности для информационно-технического воздействия со стороны злоумышленников.

На сегодняшний день организациям сложно обойтись без использования информационных систем. В связи с этим возникает вопрос о безопасности данных систем. Современные информационные системы включают в себя большое количество пользователей и данных, которые они обрабатывают. В таких системах каждую секунду выполняется достаточно большой набор различных задач. Возникающие при этом информационные потоки очень сложно отследить. Часто в таких системах возникают инциденты, приводящие к проблемам информационной безопасности.

Сегодня информация представляет собой совокупность данных предприятия и имеет высокую коммерческую ценность. Более того, при бережном отношении к информации решаются любые проблемы или заведомо предотвращаются риски, влияющие на устойчивость бизнеса.

НПО "ОнЛайн Защита" предоставляет весь комплекс услуги в области информационной безопасности и защиты информационных систем от внутренних и внешних угроз. В комплекс услуг входят:

Аудит информационной безопасности – всестороннее обследование, позволяющее показать текущий уровень защищенности информации в организации и выработать рекомендации по улучшению информационной безопасности. При проведении аудита обследуются организационные, технические, и программно-технические методы защиты информации, что позволяет учесть все возможные угрозы для организации. Аудит помещений – проверка помещений на факт наличия средств негласного съема информации (жучки, скрытые видеокамеры и пр.);

Построение процессов управления информационной безопасностью - разработка политики, концепции информационной безопасности, построение процесса реагирования на инциденты информационной безопасности, управления непрерывностью бизнеса, управления

рисками и построение процесса постоянного повышения квалификации сотрудников в области информационной безопасности;

Поставка, установка, настройка и сопровождение программных и технических средств защиты информации.

Аудит информационной безопасности

Аудит информационной безопасности помогает определить все возможные источники угроз, выявить уровень их критичности для бизнеса.

Внутренний аудит информационной безопасности всегда более эффективен, когда им занимаются профессионалы, а не сотрудники компании. У приглашенной компании более широкие знания и навыки, более совершенные инструменты для проведения внутреннего аудита информационной безопасности. И более того, уровень ответственности приглашенной компании выше уровня ответственности сотрудников. Поэтому внутренний аудит информационной безопасности от **НПО "ОнЛайн Защита"** станет качественной защитой Вашего бизнеса.

Аудит информационной безопасности предприятия – это тщательная проверка состояния корпоративных сетей и веб ресурсов.

Аудит безопасности информационных систем осуществляется с использованием автоматизированной системы поиска уязвимостей.

Результаты сканирования позволяют определить источники уязвимости сетевых ресурсов, их критичность, и проанализировать возможные последствия этих угроз.

В отчете по итогам аудита безопасности информационных систем передаются все рекомендации по устранению уязвимостей сети и сетевых ресурсов.

При желании с **НПО "ОнЛайн Защита"** подписывается договор на дальнейшее обслуживание, в рамках которого состояние защищенности сетевых ресурсов приводится в полное соответствие стандартам.

Типы аудита безопасности информационных систем, проводимые **Научно-производственным объединением "ОнЛайн Защита"**:

Экспертный аудит информационной безопасности. Дает возможность клиенту самостоятельно определить наиболее критичные для бизнес процесса информационные системы или их части. Проверка уязвимости проводится в рамках выбранных клиентом ресурсов и позволяет отказаться от комплексного аудита.

Комплексный аудит информационной безопасности. В рамках комплексного аудита информационной безопасности предприятия проводится полная проверка всех информационных ресурсов предприятия, их систем, действий персонала, внутренних и внешних

угроз. В комплексный аудит входит: экспертный анализ, аудит веб безопасности, тест на проникновение.

Аудит веб безопасности. Тщательный аудит сайтов и веб приложений компании позволяет в краткие сроки предотвратить угрозы атак на информационные системы, которые выполняют наиболее значительные для бизнеса функции.

Тест на проникновение (пентест). Пентест это тест на проверку защищенности информационных ресурсов, который представляет собой преднамеренную попытку взлома ресурса. По итогам теста на проникновение определяется эффективность существующих средств защиты против действий злоумышленников. Определяется уровень угрозы от подобных действий, и анализируются действия персонала.

В комплекс услуг **НПО "ОнЛайн Защита"** по Аудиту безопасности информационных систем также входят:

- Анализ информационных систем организации
- Анализ наиболее значимых частей информационных систем
- Анализ критичностей для информационных активов предприятия
- Автоматизированный поиск уязвимостей
- Оценка текущего состояния
- Моделирование угроз
- Определение требований к безопасности информационной среды
- Разработка рекомендаций по устранению обнаруженных уязвимостей
- Создание отчетной рекомендации
- Оценка поведения сотрудников

При проведении аудита безопасности информационных систем подписывается Соглашение о неразглашении (NDA).

Подготовка к сертификации ISO

Международный стандарт ISO/IEC 27001:2005 – самый авторитетный и универсальный из используемых стандартов информационной безопасности на предприятии.

Система информационной безопасности, соответствующая данному стандарту, не только существенно снизит все финансовые риски организации в информационной защите, но и повысит ее конкурентоспособность.

НПО "ОнЛайн Защита" оказывает услуги по подготовке системы информационной безопасности в организациях к прохождению сертификации ISO.

Построение и внедрение процессов управления информационной безопасностью

Система управления информационной безопасностью

Управление информационной безопасностью при правильном подходе может быть незаметно постороннему глазу и даже сотрудникам компании. Сделать весь процесс управления информационной безопасностью максимально комфортным и внедрить этот процесс в жизнь организации безболезненно – основной принцип работы **НПО "ОнЛайн Защита"**.

Разработка политики информационной безопасности

Управление информационной безопасностью заключается в составлении определенных норм деятельности объектов бизнеса, направленных на защиту информационных ресурсов компании, и внедрение этих норм путем создания системы информационной безопасности.

Политика информационной безопасности – это высокоуровневый документ, это система управления информационной безопасностью организации в контексте ее развития.

В идеальном варианте усилия по организации информационной безопасности и разработке политики информационной безопасности должны быть предприняты еще до момента официальной регистрации предприятия. Однако в бизнесе чаще всего наблюдается обратная ситуация. Даже во время планового развития организации зачастую не применяется никаких мер по управлению информационной безопасностью, которой должно уделяться не меньше внимания, чем стратегическому планированию бизнеса.

Стратегическое планирование в бизнесе позволяет объединить воедино маркетинговые, финансовые и производственные показатели работы компании и выстроить основные бизнес процессы с расчетом на достижение более эффективных результатов и ускорения темпов развития бизнеса. Подобное планирование становится наиболее эффективным, когда проводится совместно с организацией информационной безопасности.

Учет требований политики информационной безопасности в развитии организации необходимо пересматривать для достижения целей и задач компании на каждом этапе ее развития, но на этапах среднесрочного и долгосрочного планирования без организации информационной безопасности уже не обойтись.

Политика информационной безопасности обеспечивает защиту информационных ресурсов, утеря которых может привести к гибели компании. Организация информационной безопасности, внедряемая **НПО "ОнЛайн Защита"**, в полной мере обеспечивает надежную защиту от угроз.

В рамках организации информационной безопасности принимаются все меры для защиты информационных ресурсов.

В рамках разработки Политики информационной безопасности создается пакет следующих документов:

- Политика информационной безопасности
- Регламенты информационной безопасности
- Инструкции по обеспечению информационной безопасности для должностных лиц
- Низкоуровневые руководящие документы: отчеты, регистрационные журналы и пр.
- Прочие документы, необходимость в которых определяется на этапе аудита информационной безопасности.

Управление процессом осведомленности пользователей

Человеческий фактор является самым неконтролируемым в системе обеспечения информационной безопасности. И для уменьшения уровня воздействия этого фактора на состояние бизнеса, **НПО "ОнЛайн Защита"** проводит обучение и инструктаж сотрудников компании по вопросам обеспечения информационной безопасности на предприятии по специально разработанным программам.

Управление рисками информационной безопасности

Для качественного управления рисками информационной безопасности необходимо определить все критичные активы организации. После анализа активов и информационных систем, обеспечивающих их стабильность и сохранность, моделируется взаимодействие бизнес процессов и безопасности информационных систем с целью минимизации рисков.

Управление уязвимостями

Уязвимость информационных потоков часто не заметна взгляду, но появление новой вирусной программы может стать угрозой для части информационной системы. Проблему решает непрерывная система мониторинга уязвимостей в системе управления информационной безопасности.

Вы достигаете целей бизнеса, работая с информацией, а мы работаем с безопасностью информации, чтобы вы достигали целей бизнеса.

Внедрение систем и средств защиты информации

Современный рынок средств защиты информации, довольно, широк. Присутствие на рынке большого количества средств защиты, в совокупности с разнообразием методов, используемых в них, делают выбор подходящего средства уделом профессионалов. Ориентируясь лишь на коммерческие предложения фирм — разработчиков, вы рискуете выбрать совсем не то, что вам необходимо.

Защита любого актива, в том числе информации, основывается на выявлении наиболее вероятных угроз безопасности. Угрозы принято подразделять на внутренние и внешние. Построение комплексной системы защиты, невозможно, без учета обоих видов угроз.

Защита информации от внутренних угроз

Внутренние угрозы информационной безопасности могут быть не только умышленными (кражи, мошенничество, шпионаж), но и случайными, в случае, если их причиной стала элементарная невнимательность или халатность. Независимо от причины возникновения внутренних угроз, существуют универсальные средства защиты от них.

В качестве средства обеспечения конфиденциальности и защиты от утечек информации, наши специалисты предлагают внедрение специализированных DLP-систем. Системы такого типа препятствуют утечкам в процессе хранения, передачи и использования информации. При возникновении инцидентов, такая система может стать надежным источником для доказательств.

Внедрение DLP-систем обеспечивает централизованный контроль не только над каналами передачи информации, но и над конечными точками хранения и местами её обработки. DLP-системы позволят обезопасить использование сменных носителей информации в Вашей Компании, путем задания соответствующей политики доступа и механизмов шифрования.

Большинство, а точнее сказать, все информационные системы имеют уязвимости. Управление уязвимостями является обязательным процессом обеспечения информационной безопасности и существенно облегчается при использовании специализированных комплексных систем определения уязвимостей и реагирования на их обнаружение. Дополнительным плюсом внедрения такой системы является централизованная система отчетности, облегчающая работу руководителя отдела IT и руководству организации.

В качестве защиты от утечек информации через средства печатной и копировально-множительной техники **НПО "ОнЛайн Защита"** предлагает автоматизированный программно-аппаратный комплекс учета печати и мониторинга.

Защита информации от внешних угроз

Внешние угрозы безопасности информации Компании, такие как: распространение вирусов, шпионских программ, рассылка спама, кибер-атаки, ведут к сбоям в работе информационных систем и нарушению конфиденциальности информации.

Защита от этих угроз должна строиться комплексно и предусматривать защиту периметра организации, защиту от вредоносного кода и спама, а также защиту конфиденциальности при хранении и передаче.

Для защиты периметра используются специализированные средства, такие как: системы обнаружения и предотвращения вторжений (IDS/IPS), программно-аппаратные комплексы защиты от атак отказа в обслуживании (Dos/DDos), средства межсетевого экранирования.

В настоящее время, практически повсеместно используются средства антивирусной защиты и защиты от спама, но если об антивирусах большинство специалистов осведомлены в достаточной мере, то системы контентной фильтрации трафика и системы защиты от спама применяются не везде.

Все вышеуказанные средства становятся абсолютно бесполезны, без применения средств обеспечения конфиденциальности информации. Их использование должно проводиться комплексно и защищать информацию как при хранении (шифрование носителей информации), так и при передаче (организация VPN, SSL, ЭЦП, PKI) информации.

Большинство средств защиты способны обеспечить её сразу по нескольким направлениям, поэтому при подборе средств защиты необходимо учитывать уже существующие средства и придерживаться принципа целесообразности.

Специалисты **НПО "ОнЛайн Защита"** помогут Вам не только определиться с подходящими средствами защиты, но и внедрить их, ведь процесс внедрения требует не меньшего профессионализма от исполнителей. Наш опыт позволит выполнить работу любой сложности и в кратчайшие сроки. Не стоит откладывать обеспечение защиты на будущее или полагаться на «авось». Такой подход зачастую приводит не только к большим затратам при устранении последствий, но может негативно сказаться на имидже и репутации Компании.

Если у Вас возникли дополнительные вопросы, связаться с нами можно по телефону: +7(843)5-620-630

Или написать письмо на электронную почту: info@onlinesec.ru