ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЛАНИТ предлагает широкий спектр услуг и решений по информационной безопасности, позволяющий реализовать полный цикл работ по построению инфраструктуры информационной безопасности на предприятии. Многолетний проектный опыт и высокая квалификация специалистов ЛАНИТ гарантируют выполнение необходимого комплекса работ в поставленные сроки, с должным качеством и эффективным использованием финансовых ресурсов.

- Аудит и консалтинг в области информационной безопасности;
- внедрение систем менеджмента на основе ISO/IEC 27001;
- разработка нормативной и организационно-распорядительной документации;
- обеспечение непрерывности бизнеса на основе ISO 22301;
- защита персональных данных;
- консалтинг организаций по подготовке к процедурам лицензирования;
- организация проведения процедур сертификации, аттестации объектов информатизации, специальных исследований и специальных проверок технических средств;
- внедрение комплекса технических средств защиты информации;
- информационная безопасность промышленных систем.

Компания ЛАНИТ имеет лицензии ФСТЭК России, ФСБ России на предоставление услуг в сфере информационной безопасности.

Центр компетенции систем информационной безопасности ЛАНИТ

- Оптимизация существующей инфраструктуры заказчика на основе передовых технологий;
- поддержка при выборе технических решений;
- тестирование выбранных решений и апробация оптимальных схем реализации на этапе внедрения;
- тестирование новых решений ведущих мировых производителей.

КОМПЛЕКС УСЛУГ

Аудит и консалтинг в области информационной безопасности

Аудит представляет собой всестороннее обследование, позволяющее оценить текущее состояние информационной безопасности организации и спланировать дальнейшие шаги по повышению уровня защищенности. Аудит может проводиться как для всей компании, так и для отдельных критичных информационных систем или бизнес-процессов.

ЛАНИТ

Внедрение систем менеджмента на основе ISO/IEC 27001

ЛАНИТ предоставляет услуги по созданию в организации системы управления информационной безопасностью и ее подготовке к прохождению сертификационного аудита Британского института стандартов (BSI) или другой уполномоченной организации.

Получение сертификата BSI означает для компании не только признание высокого уровня организации информационной безопасности, но при прочих равных условиях является неоспоримым конкурентным преимуществом перед другими компаниями, особенно в нынешних условиях непрерывного роста угроз безопасности.

Разработка и внедрение организационно-распорядительных и нормативных документов в сфере ИБ

ЛАНИТ предлагает услуги опытных специалистов, которые разработают организационно-распорядительную документацию: политики по отдельным направлениям, процедуры, регламенты, инструкции, представляющие в совокупности пакет документов системы защиты информации.

Документы создаются согласно требованиям международных стандартов по информационной безопасности и руководящих документов ФСТЭК России и других регуляторов в области защиты информации.

Обеспечение непрерывности бизнеса на основе BS ISO 22301

- Проектирование отказоустойчивых схем функционирования ИТ-инфраструктуры и их тестирование в рамках пилотных проектов;
- внедрение отказоустойчивых схем функционирования ИТ-инфраструктуры;
- разработка регламентной документации по переходу на резервные мощности в случае сбоев в работе ИТ-инфраструктуры;
- тестирование механизма перехода на резервные мощности ИТ-инфраструктуры с точки зрения обеспечения непрерывности бизнес-процессов;
- формализация процесса обеспечения непрерывности функционирования ИТ-инфраструктуры и внедрение технологической системы управления непрерывностью деятельности (Business Continuity Management - BCM) для защиты ключевых бизнес-процессов компании от чрезвычайных ситуаций.

Защита персональных данных

- Полный комплекс услуг по реализации требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- срочная подготовка компаний к проверке соответствия обработки персональных данных требованиям российского законодательства в данной сфере со стороны регуляторов.

Консалтинг организаций по подготовке к процедурам лицензирования

ЛАНИТ оказывает консультационные услуги по подготовке нормативно-методической и организационно-распорядительной документации, а также проводит проверку выполнения других требований к лицензиату по соответствующим видам деятельности со стороны регуляторов в области информационной безопасности.

Организация проведения процедур сертификации, аттестации объектов информатизации, специальных исследований и специальных проверок технических средств

ЛАНИТ оказывает услуги по проведению:

- сертификационных испытаний средств защиты информации на соответствие руководящим документам ФСТЭК России;
- аттестационных испытаний автоматизированных систем на соответствие руководящим документам ФСТЭК России;
- специальных лабораторных исследований и проверок технических средств.

Информационная безопасность промышленных систем

Информация, обрабатываемая автоматизированными системами управления технологическими процессами (АСУ ТП), является критичной для обеспечения эффективности, непрерывности и безопасности промышленного процесса.

ЛАНИТ использует комплексный подход к защите промышленных систем, обеспечивая безопасность на всех уровнях архитектуры АСУ ТП.

Используемые средства обеспечения интегрируются в единую систему управления безопасностью и включают:

- межсетевые экраны (FW);
- средства предотвращения вторжений (IPS);
- сканеры уязвимостей (VA);
- системы мониторинга событий ИБ (SIEM);
- виртуальные частные сети (VPN);
- антивирусные средства (AV);
- системы контроля и управления доступом (ACS).

ЛАНИТ ПРЕДЛАГАЕТ ШИРОКИЙ СПЕКТР РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Защита периметра и каналов связи**

  Решения в области защиты периметра и каналов передачи данных предназначены для любых организаций малого, среднего и крупного бизнеса. Реализация подобного рода технологических решений опирается на функционал таких базовых средств защиты информации, как межсетевые экраны, средства обнаружения и предотвращения вторжений, VPN-концентраторы.

- **Предотвращение утечки данных**

  Для эффективного обнаружения и предотвращения утечек конфиденциальной информации компаниям требуются решения класса DLP (Data leakage prevention). Современные DLP-системы позволяют выявлять и пресекать утечку данных по всем техническим каналам – через прокси-серверы, почтовые серверы, каналы мессенджеров (в т.ч. Skype), сетевые принтеры, съемные носители информации.

> Контроль и фильтрация трафика

Фильтрация трафика позволяет принимать решение о легитимности на основе анализа его содержимого, а не на основе адресов источника или получателя. Подобный подход позволяет более гибко и точно организовать фильтрацию, предоставляя практически полный контроль над mail- и web-трафиком сотрудников и серверов, а также использованием приложений, в сочетании с комплексной антивирусной защитой.

> Центр управления информационной безопасностью (SOC)

Центр управления информационной безопасностью (Security Operation Centre) позволяет осуществлять централизованное управление информационной безопасностью в компании. Организуя разумный баланс технологий, процессов и людских ресурсов, центр предоставляет возможность непрерывного мониторинга корпоративной информационной системы, отслеживания инцидентов в сфере безопасности и быстрого реагирования на угрозы.

> Управление идентификацией и доступом (IAM)

Системы управления идентификационными данными (IAM) в основном востребованы компаниями, у которых существует большое количество прикладных ИТ-продуктов и имеется разветвленная система авторизации пользователей. IAM-система позволяет унифицировать правила доступа сотрудников ко всем информационным ресурсам организации, а также автоматизировать процессы наделения/лишения правами доступа к информационным ресурсам сотрудников в зависимости от их роли.

> Обнаружение и противодействие DDoS

Для противодействия DDoS-атакам ЛАНИТ предлагает решения на базе продуктов ведущих вендоров – Radware, Arbor, которые позволяют смоделировать профили работы ИТ-системы в штатном режиме и в случае серьезных отклонений автоматически выявлять источники массовых нестандартных запросов и отклонять данные запросы, а также иные запросы с подозрительных адресов.

Партнеры ЛАНИТ:

HP Security, Intel security, BSI Management Systems, Cisco Systems, Imperva, Positive Technologies, Radware, «Код безопасности», Symantec, Websense, «Лаборатория Касперского», «С-Терра СиЭсПи», IBM security, «Аладдин Р.Д.», Checkpoint, Balabit, «Крипто-про», Bluecoat.

Среди клиентов ЛАНИТ в сфере информационной безопасности:

Центральный банк Российской Федерации, «Сбербанк России», «Мастер-Банк», «НК «РОСНЕФТЬ», «ЛУКОЙЛ-ИНФОРМ», «ТНК-ВР Менеджмент», Страховой дом «Военно-страховая компания», Российский союз автостраховщиков, «ЖАСО», Пенсионный фонд РФ, Федеральное казначейство, Высший арбитражный суд РФ, Министерство сельского хозяйства РФ, Федеральная служба государственной статистики, Федеральное космическое агентство, Министерство транспорта РФ, НИС ГЛОНАСС, Федеральная служба по гидрометеорологии и мониторингу окружающей среды и другие.

Контактная информация:

Департамент сетевой интеграции ЛАНИТ
Тел.: (495) 967-66-57
Факс: (495) 721-19-33
E-mail: solutions@lanit.ru
security@lanit.ru
www.lanit.ru