uniteller GOZNAK

Информационная безопасность

О компании

GOZNAK — Мажоритарный акционер

Sk Skolkovo — Резидент инновационного центра Сколково

ОЭЗ ИННОПОЛИС — Резидент особой экономической зоны Иннополис

РЕЕСТР РОССИЙСКОГО ПО — Платежный шлюз и продукты компании занесены в Единый реестр ПО Российской Федерации

2008 Год основания

100+ Количество сотрудников

50+ Отраслей бизнеса

5300+ Систем самообслуживания и POS-терминалов

20+ Банков-партнеров

Направления информационной безопасности

Выполнение требований законодательства

- Государственные информационные системы (149-ФЗ)
- Критическая информационная инфраструктура (187-ФЗ)
- Персональные данные (152-ФЗ)
- Финансовый сектор (Требования Банка России)
- Автоматизированные системы управления (АСУ)

Защита от угроз безопасности информации

- Защита от угроз безопасности информации
- Выявление и предотвращение утечек информации
- Расследование компьютерных инцидентов
- Построение и эксплуатация систем управления и обеспечения информационной безопасности с учетом актуальных рисков

Наши услуги

Аудит, оценка рисков

Проектирование

Тестирование
на проникновение

Оценка соответствия,
аттестация

Виртуальный директор
по информационной
безопасности vCISO

Внедрение и техническая
поддержка средств
защиты информации

Аутсорсинг
информационной
безопасности

Аудит информационной безопасности

Комплаенс (соответствие требованиям)

- Положения Банка России, ГОСТ 57580
- Требования законодательства в сфере (информационной) кибербезопасности
- Корпоративные стандарты
- ГОСТ Р ИСО/МЭК 27001

Тестирование на проникновение

- Внешней IT-инфраструктуры
- Внутренней IT-инфраструктуры
- Веб-приложений
- Комплексное с применением методов социальной инженерии

- **Результат:**

оценка текущего уровня защищенности и рекомендации для повышения уровня безопасности

Проектирование

Проектирование систем обеспечения информационной безопасности

- Моделирование угроз безопасности
- Техническое задание
- Макетирование и тестирование
- Проектирование

Результат:

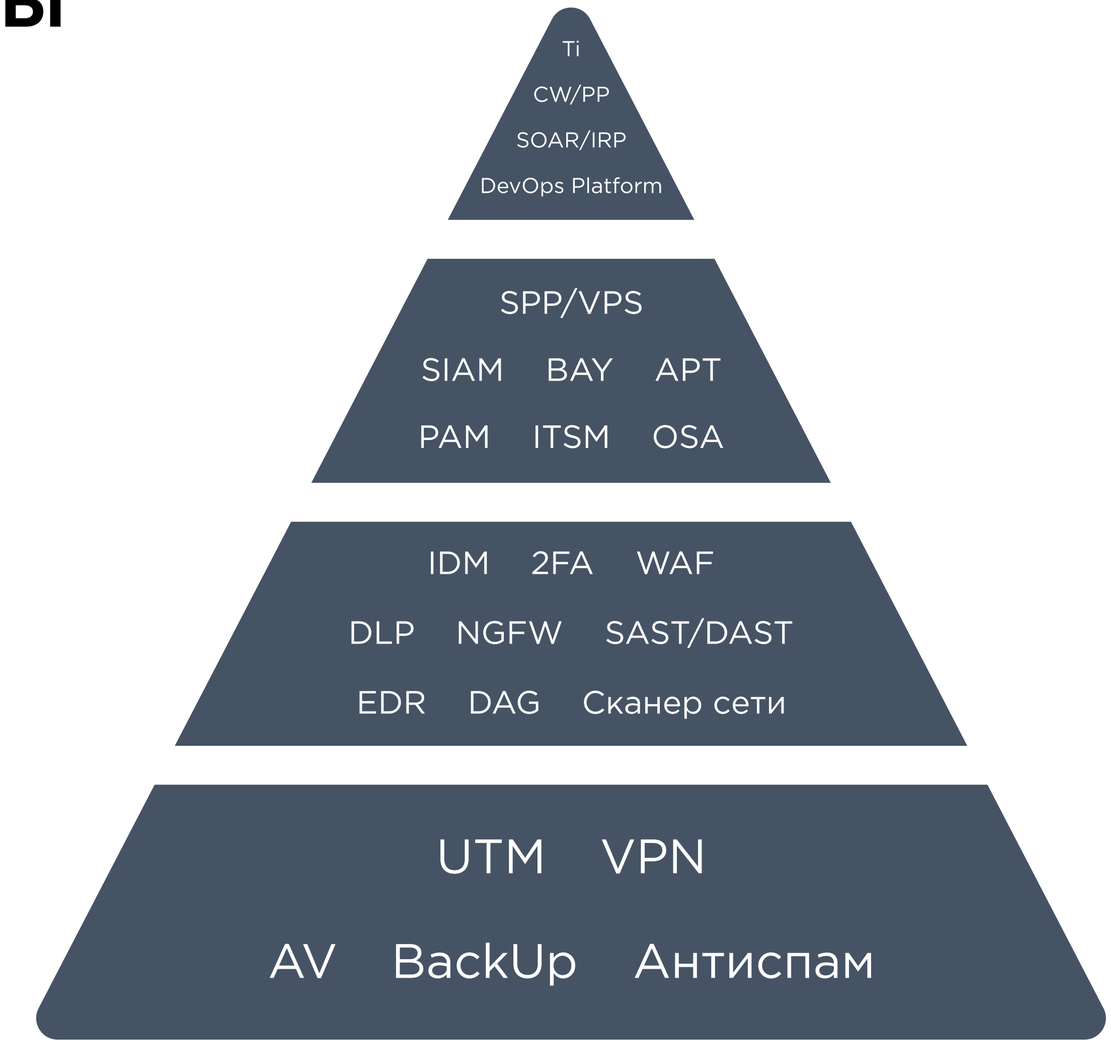
- Система защиты нейтрализует актуальные угрозы
- Она гарантированно совместима с ИТ инфраструктурой
- Учитывает возможности клиента
- Удобна для администрирования

Внедрение средств защиты

Cloud **On premise**

Результат:

- Защита от компьютерных атак
- Совместимость с ИТ инфраструктурой
- Удобство администрирования
- С учетом требований законодательства
- Оптимальное решение (цена = ценность)



Оценка соответствия

Оценка соответствия требованиям по защите информации

Аттестации информационных систем по требованиям безопасности информации

При оценке соответствия делаем первоначальное знакомство с системой и процессами обеспечения безопасности. До проведения испытаний выдаем клиентам рекомендации по устранению выявленного несоответствия, что повышает вероятность прохождения испытания.

- **Результат:** успешная оценка

Сопровождение систем защиты

Активное сопровождение - контроль работы средств защиты, тонкая настройка и выполнение плановых регламентных работ. Все самостоятельно, без напоминания клиентом.

Техническая поддержка - первая, вторая линия поддержки по средствам защиты информации.

Комплайнс - сопровождение аттестованных информационных систем, сопровождение эксплуатации средств криптографической защиты информации, внесение изменений в техническую документацию на системы защиты при изменениях в нормативно-правовых актах, при модернизации информационных системах.

- **Результат:** непрерывная и эффективная работа систем защиты

Безопасность критической информационной инфраструктуры (187-ФЗ)

- Категорируем объекты критической информационной инфраструктуры (ОКИИ)
- Проектируем системы безопасности ОКИИ
- Внедряем средства защиты информации
- Подключаем к ГосСОПКА
- Сопровождаем при проверках ФСТЭК и ФСБ

Результат:

- Выполнение работ по построению системы защиты ОКИИ
- Минимизация рисков нанесения ущерба в результате компьютерных инцидентов
- Успешное прохождение проверок надзорных органов

Безопасность персональных данных (152-ФЗ)

- Разработка организационно-распорядительной документации
- Работа с запросами субъектов персональными данными, органами контроля и надзора
- Поддержание документации по обработке персональных данных, согласий, уведомлений в актуальном состоянии
- Проектирование систем защиты персональных данных
- Моделирование угроз безопасности персональных данных
- Оценка эффективности мер защиты персональных данных в соответствие с Приказом ФСТЭК 21 и Постановлением Правительства 1119

Результат:

Соответствие требованиям законодательства
Успешное прохождение проверок надзорных органов Оперативное реагирование на инциденты

Продакт-кит

Безопасность инфраструктуры

Межсетевое экранирование (FW/UTM/NGFW)

- Континент 4
- UserGate
- ViPNet xFirewall
- С-Терра Шлюз
- Ideco UTM
- Dionis DPS
- Diamond VPN/FW
- ЗАСТАВА

Системы обнаружения и предотвращения вторжений (IDS/IPS)

- Континент СОВ
- ViPNet IDS
- С-Терра СОВ
- PT NAD

Обнаружение и защита от DDoS-атак (Anti-DDoS)	Гарда Периметр БИФИТ Митигатор
Защита виртуальных сред	vGate Базис-Virtual Security
Песочница, защита от таргетированных атак (Anti-APT)	Kaspersky Anti Targeted Attack PT Sandbox + PT NAD

Защита среды контейнеризации

- Luntry

Анализ уязвимостей (VM)

- MaxPatrol VM
- MaxPatrol 8
- PT XSpider
- RedCheck
- Сканер ВС

Анализ сетевого трафика (NTA)

- PT NAD
- Kaspersky Anti Targeted Attack
- Гарда Монитор

Deception (DDP)

- Xello Deception

Криптошлюзы (ГОСТ)

- ViPNet Coordinator
- АПКШ Континент
- С-Терра Шлюз DP
- Diamond VPN/FW
- ЗАСТАВА

TLS-шлюзы

- Континент TLS
- ViPNet TLS Gateway
- КриптоПро nGate

Защита конечных точек

Защита конечных точек (EPP)

- Kaspersky Endpoint Security
- Kaspersky Symphony Security
- Dr.Web Enterprise Security Suite
- Secret Net Studio
- ViPNet EndPoint Protection

Продвинутая защита рабочих станций (EDR/XDR)

- Kaspersky Symphony EDR/XDR
- PT XDR

Защита мобильных устройств (MDM)

- SafePhone MDM
- ViPNet Client Mobile 2

Средства доверенной загрузки (СДЗ)

- Соболь
- Аккорд
- ViPNet SafeBoot

Средства защиты от несанкционированного доступа

- Secret Net Studio
- Secret Net LSP
- Dallas Lock

Мониторинг и управление ИБ

Управление событиями информационной безопасности (SIEM)

- MaxPatrol SIEM
- RuSIEM

Управление инцидентами (SOAR/IRP)

- R-Vision SOAR
- Security Vision SOAR

Управление процессами информационной безопасности (SGRC)

- R-Vision SGRC
- Security Vision SGRC

Приложения и данные

Защита web-приложений (WAF)	PT AF Континент WAF	SolidWall WAF
Защита баз данных (DAM/DBF)	Гарда БД	Крипто БД
Предотвращение утечек информации (DLP)	InfoWatch TM Гарда Предприятие	FalconGaze
Анализ кода приложений (SAST, DAST)	PT AI	
Защита корпоративной почты (Email Security)	Kaspersky Secure Mail Gateway Kaspersky Security для почтовых серверов	

Аутентификация и управление доступом

Многофакторная аутентификация (MFA)

- Aladdin JaCarta
- Рутокен
- Indeed Access Manager

Контроль привилегированных пользователей (PAM)

- СКДПУ НТ
- Indeed Privileged AM

Аутентификация сотрудников (SSO)

- Indeed-ID Enterprise Single Sign-On

uniteller GOZNAK

Опыт. Безопасность. Uniteller

ib@uniteller.ru

uniteller.ru