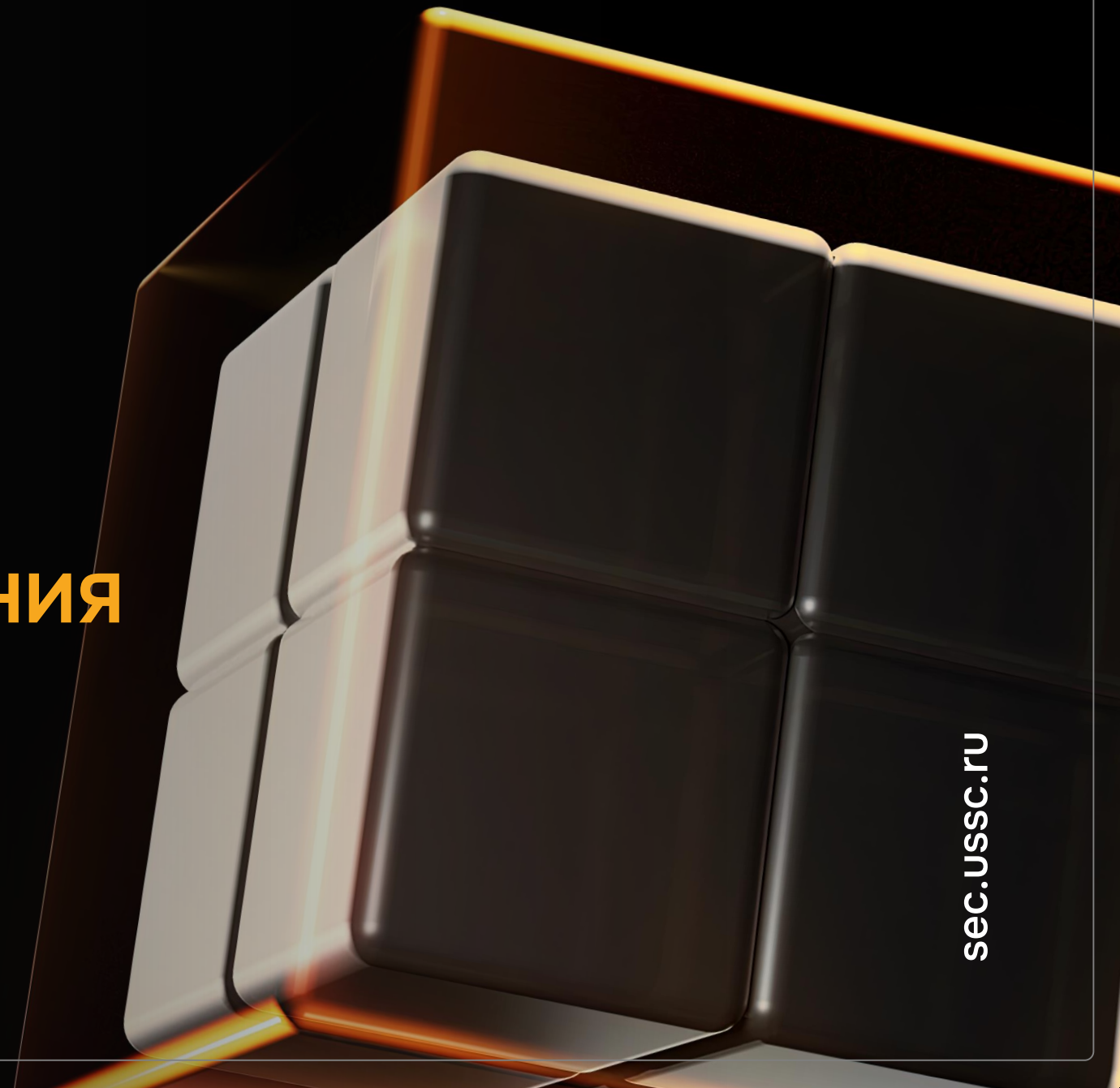
ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ



sec.ussc.ru

Система автоматизации обеспечения ИБ (САОБ)

Программный комплекс на базе ePlat4m, автоматизирующий процессы обеспечения ИБ и их интеграцию в систему управления организацией

Ключевые возможности:

- Централизованное управление и контроль процессов ИБ
- Автоматизированный контроль выполнения требований регуляторов и лучших практик в области ИБ
- Централизованный сбор данных со средств защиты информации
- Формирование отчетности, расчет метрик эффективности процессов управления ИБ

Комплекс внесен в реестр отечественного ПО — №17691 от 19.05.2023

Индивидуальный подход к автоматизации бизнеса

ГОТОВЫЕ РЕШЕНИЯ

Высокая скорость внедрения

КАСТОМИЗИРОВАННЫЕ РЕШЕНИЯ

Доработаем модули под ваши требования

ГИБКОЕ ВНЕДРЕНИЕ: КОМПЛЕКСНО ИЛИ ОТДЕЛЬНЫМИ МОДУЛЯМИ

Внедряем только необходимые модули

ВОЗМОЖНОСТИ

01. Управление активами
02. Управление критической информационной инфраструктурой
03. Управление информированием по вопросам ИБ
04. Управление обработкой персональных данных
05. Управление инцидентами ИБ
06. Моделирование угроз ИБ
07. Управление соответствием требованиям ИБ
08. Управление рисками ИБ
09. Управление мероприятиями по обеспечению ИБ
10. Управление угрозами и уязвимостями ИБ
11. Взаимодействие с НКЦКИ (ГосСОПКА)
12. Управление документами по ИБ с собственной базой знаний
13. Управление средствами защиты информации

Подберем модуль точно под ваши потребности

13 МОДУЛЕЙ*
ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ИБ

* Являются надстройкой платформы **ePlat4m**, а не ее функциями

1 МОДУЛЬ

Модуль
Управление активами

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Учет и классификация объектов защиты по уровню критичности
- Хранение, редактирование и удаление информации об объектах защиты
- Актуализация данных об ИТ-активах, а также взаимосвязей между ними
- Интеграция с внешними системами для целей автоматизированной инвентаризации и экспорта данных об ИТ-активах
- Формирование паспортов
- Ведение справочников сотрудников, бизнес-процессов и организационной структуры

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования» (п. 5.9)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Автоматизирован учет ОЗ и снижены риски утечек, оптимизированы процессы контроля безопасности

2 МОДУЛЬ

Модуль УКИИ
Управление критической информационной инфраструктурой

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Учет и категорирование ОКИИ
- Формирование и ведение реестра критически важных объектов
- Согласование и назначение ответственных по категорированию
- Автоматизация отчетности для ФСТЭК: шаблоны и заполнение документов
- Оценка выполнения приказов ФСТЭК
- Управление статусом ОКИИ: добавление и исключение из перечня

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- 187-ФЗ «О безопасности КИИ» (ст. 7)
- Постановления Правительства РФ №127 «Об утверждении Правил категорирования объектов КИИ, а также перечня показателей критериев значимости объектов КИИ и их значений»
- Приказов ФСТЭК России № 235, №236, № 239 и № 117 (в связке с модулем МУ п. 6)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Оптимизировано управление КИИ, повышен уровень защищенности

3 МОДУЛЬ

Модуль УИВИБ
Управление информированием по вопросам ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Централизованный учет сотрудников и третьих сторон
- Контроль выполнения требований ИБ:
  обучение, соглашения, доступы
- Организация процессов обучения и аттестации по вопросам ИБ

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Приказов ФСТЭК России
  - № 117 (частично: п. 56, 57)
  - № 239 (п. 13.7)
- ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования» (п. 7.2 и 7.3)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Обеспечен учет и контроль персонала с доступом к конфиденциальной информации, автоматизированы процессы обучения и проверки знаний по ИБ

4 МОДУЛЬ

Модуль УОПДн
Управление обработкой персональных данных

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Учет субъектов ПДн, ИСПДн, носителей ПДн и СрЗИ
- Наполнение и актуализация справочников ПДн
- Автоматизированное создание печатных форм и загрузка файлов в систему

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- 152-ФЗ «О персональных данных» (ст.19 ч.2 п.5)
- Постановления Правительства РФ № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн»
- Приказов ФСТЭК России
  - № 21 (п. 9, 10 и 13)
  - № 117 (п. 5)
- Приказа ФСБ России № 378 (п. 7б)
- Приказа Роскомнадзора № 179 (п. 3)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Создана единая база информации о ПДн, ИСПДн, носителях ПДн и СрЗИ

5 МОДУЛЬ

Модуль УИИБ
Управление инцидентами ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Автоматизированная обработка ИБ-событий и инцидентов
- Координация работы групп реагирования на инциденты
- Формирование типовых сценариев по реагированию и расследованию
- Интеграция с внешними системами для обмена данными
- Контроль выполнения мероприятий по реагированию и анализ принятых мер по ликвидации инцидента ИБ
- Выгрузка отчетных форм по событиям и инцидентам ИБ
- Автоматическая группировка однотипных или связанных событий ИБ в один инцидент

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Приказов ФСТЭК России
  - № 21 (п. 8.14)
  - № 31 (п. 16.6)
  - № 117 (п. 49)
  - № 239 (п. 13.5)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Обеспечено централизованное и регламентированное управление инцидентами ИБ: оперативное обнаружение, реагирование, расследование и отчетность

6 МОДУЛЬ

Модуль МУ
Моделирование угроз ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Моделирование угроз ИБ: ручное и экспертное
- Ведения и актуализации справочников угроз и уязвимостей
- Автоматизированное формирование и актуализация моделей угроз

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Приказов ФСТЭК России
  - № 117 (п.6, 11, 29а, 29в, 36)
  - № 239 (п. 11.1)
- Методики оценки УБИ ФСТЭК России от 05.02.2021

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Повышена точность оценки угроз за счет экспертных методик и упрощена подготовка к проверкам регуляторов

7 МОДУЛЬ

Модуль УСТИБ
Управление соответствием требованиям ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Централизованное хранение и обработка данных о проверках соответствия ИБ
- Автоматизация процессов оценки и контроля выполнения требований ИБ
- Управление мероприятиями по устранению несоответствий
- Расчет показателей Кзи и Пзи
- Формирование аналитической отчетности по состоянию ИБ

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- 152-ФЗ «О персональных данных» (п. 2 ч. 4 ст. 19)
- Приказов ФСТЭК России
  - № 21 (п. 6)
  - № 117 (п. 31, 32, 33)
  - № 239 (п. 13.1 и 13.8)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Обеспечен системный контроль соответствия требованиям ИБ и сокращено время проверок

8 МОДУЛЬ

Модуль УР
Управление рисками ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Комплексный анализ и учет рисков ИБ
- Автоматизированная расчет и оценка уровня рисков ИБ
- Планирование мероприятий по снижению рисков
- Автоматизированное формирование отчетов о состоянии защищенности

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска ИБ»
- ISO/IEC 27005:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по управлению рисками нарушения информационной безопасности»

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Снижено время оценки рисков за счет автоматизации и обеспечения обоснованности принимаемых решений по ИБ

9 МОДУЛЬ

Модуль УМОИБ
Управление мероприятиями по обеспечению ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Создание, контроль и учет выполнения поручений и мероприятий
- Организация работы исполнителей с установленными сроками и приоритетами
- Формирование и управления планами мероприятий
- Визуализация статусов и показателей выполнения

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Приказа ФСТЭК России № 117 (п. 33 - частично)
- Внутренних регламентов по документообороту и управлению задачами
- Отраслевых стандартов (при наличии) по контролю исполнения поручений
- Политик корпоративного управления в части отчетности и KPI

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Оптимизировано планирование мероприятий и их привязка к другим объектам системы, обеспечена прозрачность выполнения задач для руководства

10 МОДУЛЬ

Модуль УУУИБ
Управление угрозами и уязвимостями ИБ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Регистрация и хранение сведений об угрозах и уязвимостях ИБ
- Автоматизированный сбор данных из внутренних систем мониторинга
- Формирование планов устранения угроз и уязвимостей ИБ
- Выполнение мероприятий по устранению угроз и уязвимостей
- Интеграция с внешними сканерами безопасности по поиску угроз и уязвимостей
- Мониторинг уязвимостей и оценка их применимости на основании данных из внешних и внутренних источников (например, из ФСТЭК)

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Приказов ФСТЭК России
  - № 21 (п. 3)
  - № 239 (п. 11.1, 12.6)
  - № 117 (п. 38 - частично)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Сформирована единая база угроз и уязвимостей ИБ организации, контроль выполнения и эффективности защитных мероприятий

11 МОДУЛЬ

Модуль взаимодействия с НКЦКИ (ГОССОПКА)
Передача отчетности об инцидентах ИБ в НКЦКИ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Ведение реестра субъектов КИИ и относящихся к ним объектов
- Регистрация, реагирование и расследование инцидентов ИБ
- Интеграция с SIEM для импорта информации об инцидентах ИБ
- Реализация автоматизированного обмена информацией на основе программного интерфейса (посредством API)

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- 152-ФЗ «О персональных данных» (ч. 12 ст. 19)
- 187-ФЗ «О безопасности КИИ» (ст. 9)
- Приказов ФСБ России № 77 и № 367 (приложение № 2, п. 3)
- Приказов ФСТЭК России
  - № 117 (п. 34л, 34х, 59)
  - № 239 (п. 26.2)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Обеспечена оперативная передача сведений о киберинцидентах в форматах, установленных НКЦКИ

12 МОДУЛЬ

Модуль УДИБ
Управление документами с собственной базой знаний

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Централизованное хранение и систематизация документов по ИБ
- Ведение реестра соглашений и договоров о конфиденциальности
- Управление актуальными версиями документов
- Автоматическое создание документов на базе шаблонов/данных
- Настройка уведомлений о необходимости актуализации документации
- Интеграция с системами документооборота для импорта/экспорта документов

ПОМОГАЕТ ОБЕСПЕЧИВАТЬ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования» (п. 7.5) – частично

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Создана единая база нормативных документов и справочников по ИБ, обеспечена поддержка соответствия документации текущим нормативным требованиям

13 МОДУЛЬ

Модуль УСЗИ
Управление средствами защиты информации

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Учет и хранение данных о СЗИ (включая СКЗИ)
- Мониторинг состояния СЗИ вручную и по данным внешних систем
- Учет лицензий на СЗИ и состояния их актуальности
- Назначение и контроль исполнения задач на поддержку актуального и работоспособного состояния СЗИ

АВТОМАТИЗИРУЕТ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Приказа ФСТЭК России № 117 (п. 7, 22, 23, 34, 39, 71, 72)

РЕЗУЛЬТАТ ВНЕДРЕНИЯ

Обеспечен контроль актуальности версий и работоспособности СЗИ, а также прозрачное управление жизненными циклом СЗИ

4 ключевых преимущества системы автоматизации обеспечения ИБ

Единая платформа вместо «зоопарка»: множества Excel-файлов и других способов хранения информации

Единая консоль для контроля ключевых показателей информационной безопасности

Обеспечение соответствия требованиям регулятора

Автоматизация рутинных процессов и отчётности, снижение влияния человеческого фактора

Можем интегрироваться с любой системой

Интеграции, которые уже работают*

- SIEM-системы
- DLP-решения
- IDM-системы
- ITSM-платформы
- HR-системы
- Системы аудита ИБ-защищенности
- Системы контроля конфигураций и состояний рабочей среды
- Антивирусные продукты
- Службы каталогов (Active Directory/LDAP)

* Возможно, понадобится донастройка под вашу версию внешней системы

Кейс №1: Субъект КИИ с объектами 1 категории значимости

ПОТРЕБНОСТЬ

Требуется категорирование объектов КИИ и подтверждение соответствия 187-ФЗ

ПРОБЛЕМА

Подготовка к аттестации занимает более 6 месяцев из-за следующих факторов:

- Ручная инвентаризация активов — приводит к ошибкам в 30% записей
- Разрозненные данные по угрозам — несоответствие между требованиями ФСТЭК №239, БДУ ФСТЭК России
- Отсутствие актуальных шаблонов документов для соответствия требованиям ФСТЭК России

РЕШЕНИЕ

- Автоматическая инвентаризация ОЗ (импорт из сетевых сканеров и CMDB)
- Моделирование угроз по шаблонам ФСТЭК — сокращение времени с 4 недель до 3 дней
- Генерация отчетов по 187-ФЗ (приказ №235) в один клик

РЕЗУЛЬТАТ

- ✓ Срок категорирования сокращен с 6 месяцев до 8 недель
- ✓ Сэкономлено 3,5 млн. руб. на аудиторах
- ✓ Отсутствие штрафов за 3 года

МОДУЛИ, КОТОРЫЕ ВНЕДРИЛИ

- Управление критической информационной инфраструктурой
- Учет и классификация объектов защиты
- Моделирование угроз безопасности
- Управление соответствием требованиям ИБ
- Управление документами по ИБ с собственной базой знаний

Кейс №2: Промышленная компания

ПОТРЕБНОСТЬ

Оптимизация бюджета на ИБ за счет приоритезации рисков

ПРОБЛЕМА

>20% бюджета компании уходит на неэффективные СрЗИ из-за следующих факторов:

- Отсутствия единой карты рисков — разрозненные данные в Excel
- Ручной расчет эффективности мер защиты
- Нет методики расчета экономического показателя

РЕШЕНИЕ

- Корреляция угроз, уязвимостей и активов в единой матрице
- Разработана методика расчета рисков под заказчика

РЕЗУЛЬТАТ

- ✓ Годовые затраты на ИБ снижены на 15%
- ✓ Увеличено покрытие рисков с 70% до 95%

МОДУЛИ, КОТОРЫЕ ВНЕДРИЛИ

- Управление рисками в ИБ
- Управление угрозами и уязвимостями ИБ
- Управление мероприятиями по обеспечению ИБ
- Моделирование угроз безопасности

Уральский центр систем безопасности (УЦСБ)

с 2007
экспертиза в ИТ и ИБ

> 900
профессионалов в штате

> 4000
завершенных проектов

Входим в список 100 крупнейших компаний России в сфере защиты информации и ИТ по версии CNews Analytics и TAdviser

Компетенции

- Кибербезопасность
- Информационные технологии
- Инженерно-технические системы

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

— объединение профильных компетенций УЦСБ по внедрению передовых практик и технологий для защиты критически важных систем от цифровых атак

- Банки и финансовые компании
- Госсектор
- ИТ и телеком
- Энергетика
- Металлургия
- Нефтегаз
- Транспорт
- Машиностроение
- Сельское хозяйство
- Торговля

САОБ разработан на платформе ePlat4m

Low-code платформа для быстрой разработки и автоматизации информационных систем бизнеса

Быстрая разработка

Благодаря визуальным конструкторам и готовым модулям

Безопасность

- Сертификат ФСТЭК
- Гибкое управление ролями и правами

Масштабируемость

Возможность масштабирования в соответствии с ростом бизнеса и увеличением нагрузки

С применением экспертизы аналитического центра УЦСБ

Компетенции центра

- Аудит ИБ: ПДн, КИИ, АСУТП, ГИС ISO, отраслевые и корпоративные требования
- Моделирование угроз безопасности
- Разработка ОРД
- Аттестация и категорирование
- Оценка соответствия, подготовка к проверкам регуляторов
- Консалтинг по сертификации ПО или СЗИ

Команда экспертов

Сертификация: OSCP, OSWE, OSCE, CISA, CISM, CISSP, CRISC, ISO 27001

Непрерывно следим за изменениями отраслевого законодательства и публикуемся в профильных СМИ и медиа

ePlat4m — разработка ИБ-решений с 2014 года

> 40 реализованных проектов по автоматизации управления ИБ

Полностью российская разработка: соблюдаем требования технологической безопасности и независимости КИИ (указ Президента РФ №166 от 30.03.2022)

Лицензии и сертификаты

- Сертификат соответствия ФСТЭК России на ПО ePlat4m №4433 от 29.07.2021
- Лицензии ФСТЭК и ФСБ России
  - Лицензия на деятельность по технической защите конфиденциальной информации №Л024-00107-00/00580547 от 08.10.2007
  - Лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации №Л050-00107-00/00579687 от 08.10.2007
  - Лицензия на деятельность по разработке, производству, распространению шифровальных (криптографических) средств №Л051-00105-66/00556455 от 05.08.2013

Этапы работ

1

Демонстрация продукта

- Показываем работу системы на стенде и отвечаем на все вопросы

2

Два варианта пилотирования продукта

- Внедрение готового решения, позволяющего вашей компании сразу начать работу с системой
- Внедрение кастомизированной версии продукта с доработками под конкретные требования вашей компании

3

Анализ и аудит

- Выполняется экспертами ИБ и ИТ, бизнес-аналитиками
- Учитываем лучшие практики и специфику вашей компании

4

Проектирование

- Анализируем ваши потребности и формулируем требования к системе
- Создаем и согласовываем техническое задание

5

Внедрение и интеграция

- В срок с поэтапным контролем качества на основании практик проектного управления

6

Потенциальные доработки

- Гибко, быстро, итерациями

7

Запуск обучения

- Передача опыта и знаний, подробное документирование для самостоятельной эксплуатации

8

Поддержка и развитие

- Собственный сервисный центр: быстрое реагирование, доработки по запросу

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

ОСТАВИТЬ ЗАЯВКУ НА ДЕМОНСТРАЦИЮ ПРОДУКТА

+7 (343) 379-98-34

eplat4m.ru

cybersec@ussc.ru