INNOSTAGE

CIT ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ ТАТАРСТАН

Центр предотвращения киберугроз Республики Татарстан

Шамиль Биккинин
Руководитель департамента ИБ
ЦИТ Республики Татарстан

Виктор Вячеславов
Технический директор
ГК Innostage

Кто мы

ЦИТ ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ ТАТАРСТАН

INNOSTAGE

ЦИТ ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ ТАТАРСТАН

Государственный интегратор

Контакт-центр

Обслуживание ИТИ Республики Татарстан

INNOSTAGE

Центр предотвращения киберугроз CyberART

Стратегический партнер Positive Technologies

IRP-система собственной разработки

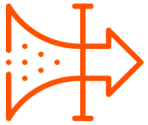
Вызовы, требующие ответа

Высокие темпы цифровизации государственных и муниципальных услуг

Рост количества кибератак на государственные ресурсы

Недостаточный уровень подготовки пользователей

Длительное реагирование на инциденты ИБ



Появление новых методов кибератак

Недопустимые риски для ГИС

Риски	Примеры причин возникновения рисков
Потеря политического доверия	• Нарушения достоверности и корректности данных • Нарушения сроков исполнения поручений • Публикации, компрометирующие первых лиц
Потеря социального доверия	• Снижение качества государственных услуг • Утечки персональных и конфиденциальных данных • Негативные публикации в результате утечек
Потеря контроля функционирования ИТ	• Остановка работы государственных органов и организаций • Взлом и недоступность государственных ИТ-сервисов
Потеря финансовой стабильности	• Нецелевое использование денежных средств • Неисполнение бюджета • Мошенничество с финансовыми показателями

Выбор подхода к созданию ЦПК

Регуляторная безопасность

- ФСТЭК, ФСБ, ЦБ РФ
- Отраслевые стандарты
- Стандарты компании

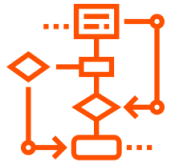
Практическая безопасность

- Недопустимые события
- Верификация рисков
- Построение Центра предотвращения киберугроз
- Сокращение поверхности атак
- Регулярные киберучения и верификация защищенности

Цели создания ЦПК

Регулярная проверка эффективности мер киберзащиты

Обеспечение безопасного функционирования ключевых процессов и ГИС



Расследование инцидентов ИБ

Централизация ресурсов и практической экспертизы

Обнаружение компьютерных атак и нарушений

Модель построения ЦПК

Входные условия

- Результат «в железе» должен быть до конца года
- Кадровый дефицит квалифицированных специалистов
- ЦИТ РТ должен быть «владельцем» основных процессов и взять на себя всю эксплуатацию в течение 3х лет

Выбрана гибридная модель построения ЦПК

Архитектура ЦПК

Центр предотвращения киберугроз (ЦПК)

централизация, систематизация и автоматизация деятельности по обеспечению практической защиты

Обнаружить злоумышленника, движущегося к реализации недопустимого события, за время,достаточное для предотвращения атаки

Злоумышленник

Негативное воздействие на любом из уровней

Защищаемый объект

Уровень субъекта (обсл. персонал/пользователи)

- Уровень данных и информационных потоков
- Прикладной уровень
- Уровень узла
- Уровень сети
- Уровень инфраструктуры и средств защиты информации

Сенсоры ЦПК уровня объекта

- Сенсоры контроля субъектов 2FA-Sensor (2FA)
- Сенсоры контроля каналов передачи данных Data-Leak-Sensor (DLP)
- Сенсоры контроля каналов прикладного уровня Web-Sensor (AF)
- Сенсоры контроля узла OS (EDR/XDR)
- Сенсоры контроля сети NET-Sensor (NTA/IDS)
- Сенсоры контроля журналов событий Log-Event-Sensor (LM/SIEM)

Сенсоры контроля активов и уязвимостей Vulnerability-Sensor (NetScaner/VM)

Ядро ЦПК

- Средства управления активами (IRP/CMDB)
- Средства управления уязвимостями (VM)
- Средства управления инцидентами (IRP)
- Средства управления событиями безопасности (LM/SIEM/ML)
- Средства контроля работоспособности (BAS/IT-Monitoring)
- Средства взаимодействия (TiketingSystem/KB)
- Средства реагирования на инциденты (SOAR)

Персонал ЦПК

Сенсоры ЦПК централизованного контроля

- Сенсоры контроля файлов FS-Sensor (AV/Sandbox)
- Сенсоры контроля индикаторов компрометации TI-Sensor (TIP)
- Сенсоры контроля угроз ловушки (DDP)

Архитектура ЦПК

Центр предотвращения киберугроз (ЦПК)

централизация, систематизация и автоматизация деятельности по обеспечению практической защиты

Обнаружить злоумышленника, движущегося к реализации недопустимого события, за время,достаточное для предотвращения атаки

Злоумышленник

Негативное воздействие на любом из уровней

Защищаемый объект

Уровень субъекта (обсл. персонал/пользователи)

- Уровень данных и информационных потоков
- Прикладной уровень
- Уровень узла
- Уровень сети
- Уровень инфраструктуры и средств защиты информации

Сенсоры ЦПК уровня объекта

- Сенсоры контроля субъектов 2FA-Sensor (2FA)
- Сенсоры контроля каналов передачи данных Data-Leak-Sensor (DLP)
- Сенсоры контроля каналов прикладного уровня Web-Sensor (AF)
- Сенсоры контроля узла OS (EDR/XDR)
- Сенсоры контроля сети NET-Sensor (NTA/IDS)
- Сенсоры контроля журналов событий Log-Event-Sensor (LM/SIEM)

Сенсоры контроля активов и уязвимостей Vulnerability-Sensor (NetScaner/VM)

Ядро ЦПК

- Средства управления активами (IRP/CMDB)
- Средства управления уязвимостями (VM)
- Средства управления инцидентами (IRP)
- Средства управления событиями безопасности (LM/SIEM/ML)
- Средства контроля работоспособности (BAS/IT-Monitoring)
- Средства взаимодействия (TiketingSystem/KB)
- Средства реагирования на инциденты (SOAR)

Персонал ЦПК
10 чел.

Сенсоры ЦПК централизованного контроля

- Сенсоры контроля файлов FS-Sensor (AV/Sandbox)
- Сенсоры контроля индикаторов компрометации TI-Sensor (TIP)
- Сенсоры контроля угроз ловушки (DDP)

Старт проекта

1. Разработка и защита концепции построения Центра предотвращения киберугроз

2. Заключение соглашения о сотрудничестве между Республикой Татарстан и компанией Positive Technologies

3. Проектирование и реализация технических решений первого пускового комплекса

Дорожная карта создания ЦПК

1 Первый год

- Разработка дизайна и архитектуры
- Пилотирование технических средств
- Проектирование первого комплекса программно-технических средств
- Внедрение базовых компонентов ЦПК

2 Второй год

- Обучение и проверка экспертизы персонала
- Разработка и реализация процессов
- Проектирование и внедрение дополнительных программно-технических средств
- Самостоятельный мониторинг и анализ инцидентов ИБ 24/7

3 Третий год

- Доработка, адаптация и повышение эффективности процессов
- Масштабирование и развитие программно-технических средств
- Поддержка и развитие аналитического контента
- Киберучения для проверки эффективности работы

INNOSTAGE

CIT ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ ТАТАРСТАН

Спасибо за внимание! Вопросы?

Шамиль Биккинин
Руководитель департамента ИБ
ЦИТ Республики Татарстан

Виктор Вячеславов
Технический директор
ГК Innostage