Киберустойчивость организации.

Проблемные вопросы и возможные решения.

Акимов Сергей Леонидович

Заместитель генерального директора

ИНФОРМПРОСТРАНСТВО СЕГОДНЯ

- **Информпространство** строилось при приоритете юзабилити;
- **Новые услуги- потребность сегодняшнего дня -Взаимодействие с потребителем услуг –>–> невозможность построения «закрытой системы»**;
- Число пользователей интернета **~ 4,5 млрд**. (рост за 2017г. более 7%);
- Количество абонентов мобильной связи **> 8 млрд**. (За 2017г. В России продано более 100 млн. SIM карт);
- **Интернет сервисы и облака**: облачные технологии популярны для осуществления обслуживания клиентов (41% в России и 34% в мире) и управления финансами (37% и 32%); PwC
- 44% **(40% в России)** организаций не имеют **целостной стратегии обеспечения кибербезопасности**, (PwC, анализ трендов ИБ на 2018г).

Основные возможные последствия от атак (PwC на 2018г):

- 40% (37% в России) считают нарушение операционной деятельности;
- 39% (48%) утечку конфиденциальных данных;
- 32% (27%) нанесение вреда качеству продукции;
- 29% (30%) нанесение ущерба материальному имуществу.

«Завтра успешными государствами будут по всей вероятности те страны, которые инвестируют в инфраструктуру, знания и взаимоотношения, и которые устойчивы к потрясениям,- будь то экономические, экологические, общественные или кибернетические». (Отчет Сената национальной разведки США, 2017г.)

ТРЕБОВАНИЯ К УСТОЙЧИВОСТИ КИБЕРНЕТИЧЕСКОЙ СИСТЕМЫ

- непрерывность;
- оперативность;
- конфиденциальность/целостность;
- адаптивность к изменению условий функционирования;
- обеспечение единого информационного пространства;
- эффективность и эволюционность в развитии.

Во многом требования к КУ созвучны требованиям к ИБ и непрерывности бизнеса

ДЛЯ ИНФРАСТРУКТУРЫ ФИНАНСОВОГО РЫНКА:

- Определено понятие финансовой устойчивости;

- Предложена методика оценки финансовой устойчивости (указание от 16.01.2004 № 1379-У «Об оценке финансовой устойчивости….», а также рекомендации по алгоритму расчетов показателей финансовой устойчивости коммерческих банков);

- Определено понятие устойчивости функционирования организации в условиях кибератаки:

«Возможность прогнозировать и поглощать ущерб от кибератаки, адаптироваться и оперативно восстанавливать исходное состояние организации после негативных воздействий в результате реализации кибератаки». (Банк России. «Доклад комитета по платежам и рыночным инфраструктурам., 2014г.) «

РЕАЛИЗУЕМА ЛИ «НЕПРОБИВАЕМАЯ» СИСТЕМА?

- Цифровизация бизнеса, мобильность, коллективная работа, облачные технологии;
- Уязвимости в ПО;
- Уязвимости в сетевом оборудовании;
- Уязвимости в СЗИ;

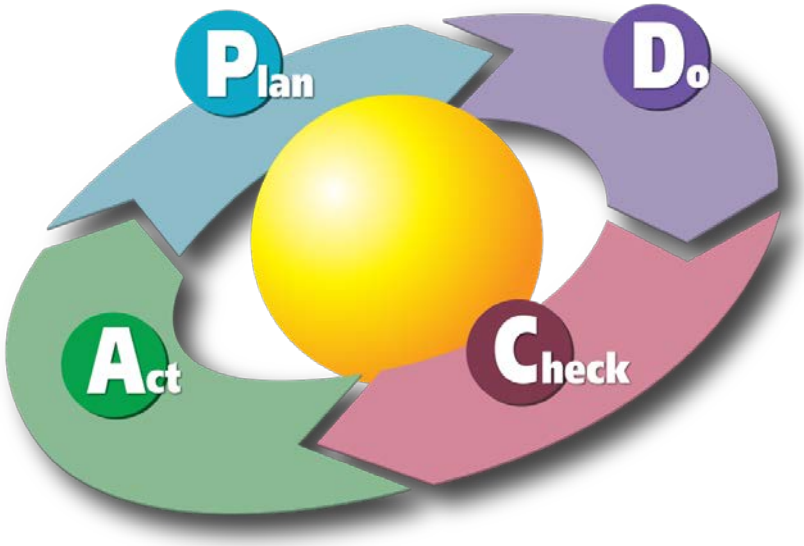
- Человеческий фактор;
- Рост числа, возможностей и квалификации атакующих;
- Развитие рынка криминальных киберуслуг ;
- Высокая мотивация атакующих

Пришло осознание - успешные кибератаки неизбежны.

Нужны другие подходы и методики!

КЛАССИЧЕСКАЯ МЕТОДОЛОГИЯ МЕНЕДЖМЕНТА ИБ (цикл Деминга)

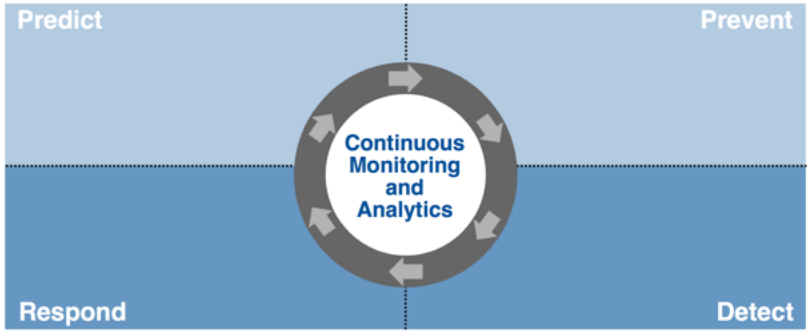
1. Планирование (Plan)
2. Выполнение (Do)
3. Проверка (Check)
4. Воздействие (Act)



МЕТОДОЛОГИЯ АДАПТИВНОЙ БЕЗОПАСНОСТИ ОТ GARTNER

1. Прогнозирование (Predict)
2. Предотвращение (Prevent)
3. Обнаружение (Detect)
4. Реакция (Respond)

The Adaptive Security Architecture



Gartner

МЕТОДОЛОГИЯ АДАПТИВНОЙ БЕЗОПАСНОСТИ ОТ GARTNER

1 Прогнозирование (Predict)

- Прогнозирование направления атак
- Проактивный анализ воздействий
- Фиксация нормальных режимов функционирования

2 Предотвращение (Prevent)

- Изолирование системы
- Блокирование злоумышленников
- Предотвращение инцидентов

3 Обнаружение (Detect)

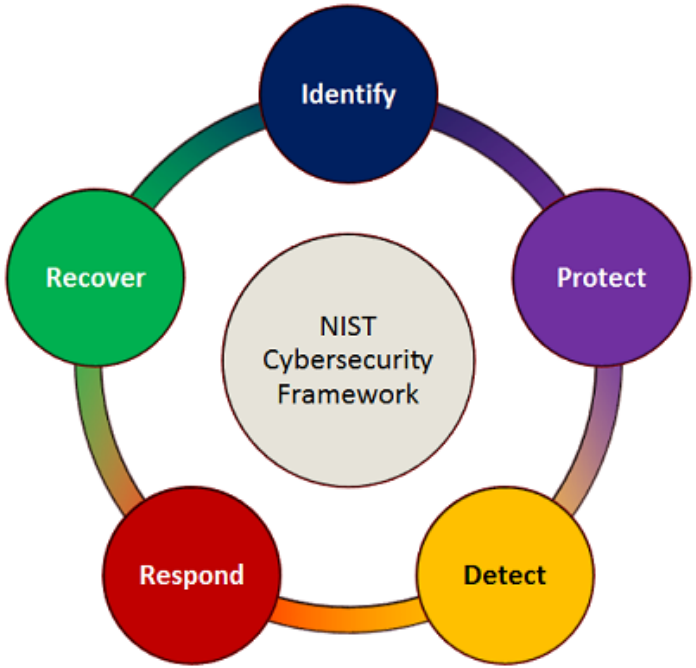
- Обнаружение инцидентов
- Подтверждение и приоритизация рисков
- Ведение реестра инцидентов

4 Реакция (Respond)

- Расследование инцидентов
- Планирование и реализация изменений
- Корректировка моделей

МЕТОДОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ ОТ NIST

1. Идентификация (Identify)
2. Защита (Protect)
3. Обнаружение (Detect)
4. Реагирование (Respond)
5. Восстановление (Recover)



МЕТОДОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ ОТ NIST

1 Идентификация (Identify)

- Управление активами
- Среда функционирования
- Требования
- Оценка рисков
- Стратегия управления рисками

2 Защита (Protect)

- Управление доступом
- Обучение и повышение осведомленности
- Защита информационных ресурсов
- Процедуры и процессы защиты информации
- Поддержка мер
- Защита процессов

3 Обнаружение (Detect)

- Аномалии и события
- Непрерывный мониторинг безопасности
- Процессы выявления инцидентов

4 Реагирование (Respond)

- Планирование реакции
- Взаимодействие и оповещения при реагировании
- Анализ выявленных инцидентов
- Минимизация негативного воздействия
- Улучшение процессов реагирования

5 Восстановление (Recover)

- Планирование восстановления
- Улучшение процессов восстановления
- Взаимодействие в процессе восстановления

План на случай непредвиденных обстоятельств – план «Б»

- Устранение негативных последствий
- Скорейшее восстановление

ПЛАН «Б» -комплекс 2х взаимозависимых блоков:

1

- Наличие соответствующих руководств и инструкций,
- Обучение,
- Подготовка персонала,
- Проведение киберучений в организации по необходимым действиям в случае успешной кибератаки и т.д..

2

- Развернутая техническая инфраструктура, адаптируемая, обеспечивающая выполнение критичных операций в условиях успешной кибератаки и последующее восстановление функционирования.

ОРГ. СОСТАВЛЯЮЩАЯ:

БАЗА для подготовки: СУЩЕСТВУЮЩАЯ НОРМАТИВНАЯ БАЗА БР ДЛЯ РАЗРАБОТКИ ПЛАНА/регламента обеспечения КИБЕРУСТОЙЧИВОСТИ:

- ПРИЛОЖЕНИЕ 5 к «Положению об организации внутреннего контроля в кредитных организациях и банковских группах». (Рекомендации по структуре и содержанию плана действий на обеспечение непрерывности…. И восстановлению….);
- ГОСТ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (определены требования к организации обеспечения непрерывности бизнеса и его восстановлению после прерываний….)
- Стандарт АРБ: «Программа управления непрерывностью деятельности кредитных организаций банковской системы Российской Федерации».

ОРГ. СОСТАВЛЯЮЩАЯ

РЕКОМЕНДАЦИИ ФОРУМА ПО НАБЛЮДЕНИЮ ЗА SWIFT РЕГЛАМЕНТА ОБЕСПЕЧЕНИЯ ПЛАНА «Б» КИБЕРУСТОЙЧИВОСТИ:

- *CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, June 2016;*
- *CPMI-IOSCO, Principles for financial market infrastructures,*
  F: Oversight expectations applicable to critical service providers;
- *CPMI, «Cyber resilience in financial market infrastructures», November 2014*

ЧАСТНЫЕ РУКОВОДСТВА FFIEC, Federal Reserve Banks;

Рекомендации международного экономического форума, январь 2017

ТЕХНИЧЕСКАЯ ИНФРАСТРУКТУРА ПЛАНА «Б»

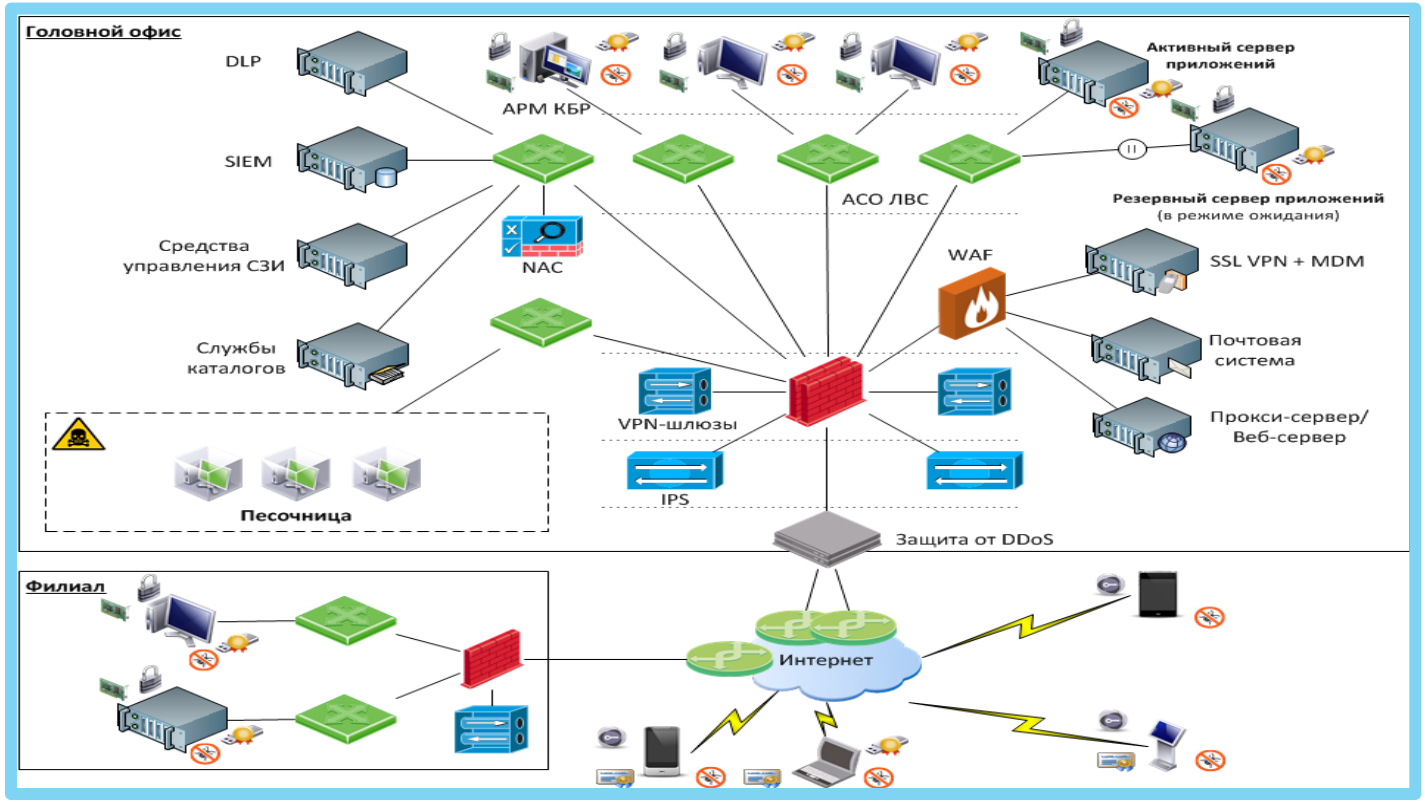
В рамках создания классических систем обеспечения информационной безопасности решаются задачи

- ПРОГНОЗИРОВАНИЕ
- ДЕТЕКТИРОВАНИЕ
- ПРЕДОТВРАЩЕНИЕ

Акценты при реализации плана «Б»

- ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ
- ВОССТАНОВЛЕНИЕ

АРХИТЕКТУРА ПРИМЕНЕНИЯ КЛАССИЧЕСКИХ СЗИ



АДАПТИВНАЯ ТКС С БЛОКИРОВКОЙ НЕДОВЕРЕННЫХ СЕГМЕНТОВ

infotecs

Архитектура должна предполагать выделение сегментов для блокирования распространения атак на случай реализации плана “Б”

Сетевые шлюзы:

- оперативная сегментация информационной инфраструктуры для повышения живучести – «защитные переборки» для блокировки распространения атаки (WB - watertight bulkhead).

Дополнительные функции управления доступом:

- оперативное (в реальном масштабе времени) переконфигурирование и изменение правил доступа.

Сервера, шлюзы, рабочие станции и мобильные устройства:

- наличие второго режима - защищенный режим «Б».

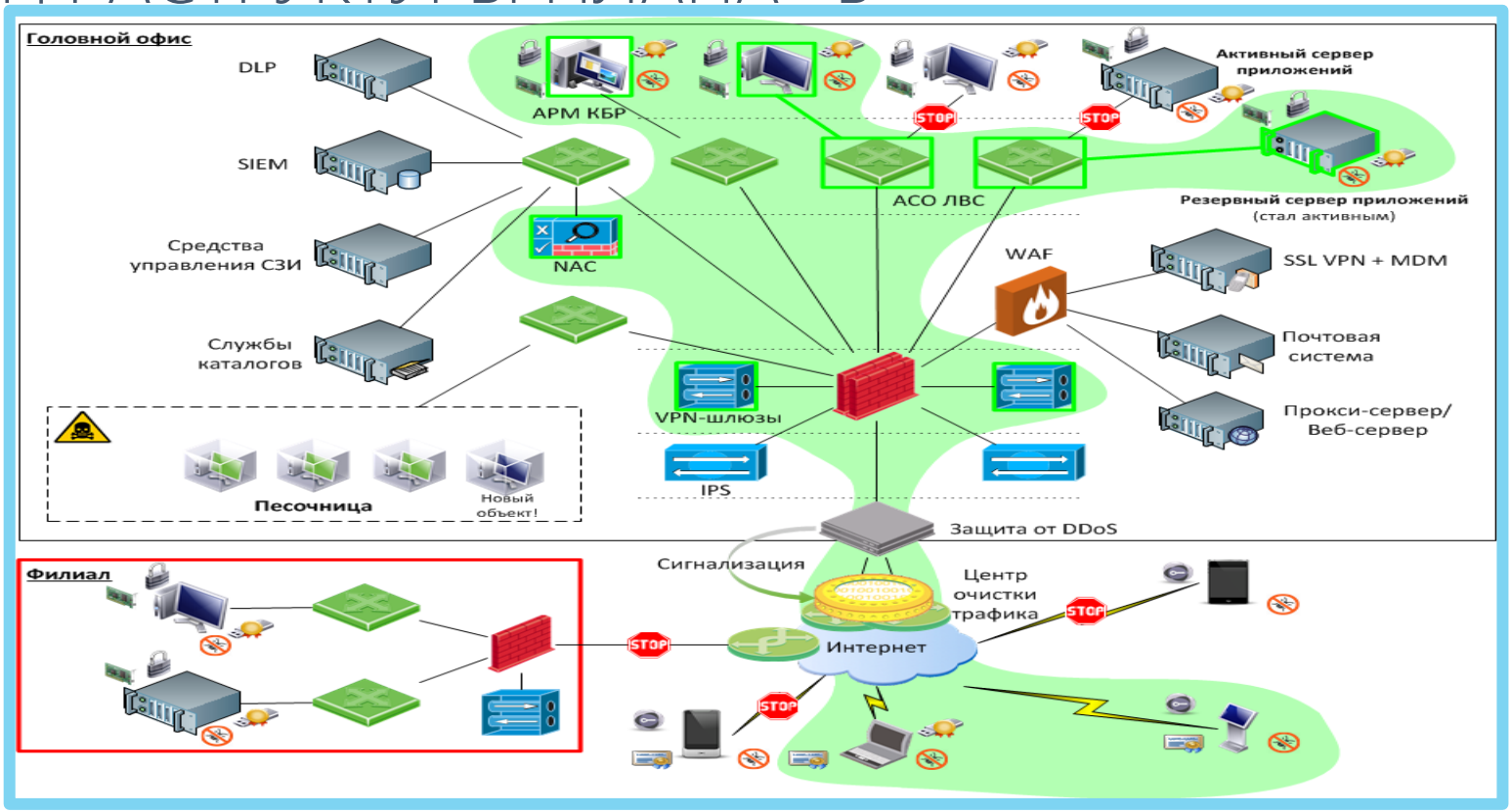
Сетевая инфраструктура:

- гарантированная доставка команд управления на критические узлы ТКС.

ПРИМЕР РЕАГИРОВАНИЯ ИНФРАСТРУКТУРЫ ПЛАНА «Б»

1. Переключение МЭ, серверов, сетевых устройств в защищенный режим «Б» (автоматически или «вручную»)
2. Отключение доступа с компрометированных точек доступа и сегментов сети, переконфигурирование сети.
3. **Создание с помощью МЭ и VPN замкнутых доверенных анклавов для выполнения критических операций**
4. Переключение (перезагрузка) терминальных стационарных и мобильных устройств в защищенный режим «Б»
5. Запрет доступа без строгой аутентификации и с устройств, не обеспечивающий полноценный контроль целостности для MDM
6. Временный запрет допуска приложений из «песочницы» и т.п.

ВИЗУАЛИЗАЦИЯ РЕАГИРОВАНИЯ ИНФРАСТРУКТУРЫ ПЛАНА «Б»



ПРОБЛЕМЫ

- **Отсутствие отечественной методической базы** для оценки уровня киберустойчивости и реализации необходимых мер по ее обеспечению;
- Планирование мероприятий и внедрение решений по КУ требует **существенных затрат**;
- Мероприятия по эффективному обеспечению КУ требуют наличия **достаточного количества подготовленных специалистов, экспертных организаций**;
- **Необходимость доверенного взаимодействия** кредитно-финансовых организаций при подготовке и реализации планов “Б”;
- Для безопасной цифровизации бизнеса и услуг нужен **кибер-просвещенный потребитель**.

КЛЮЧЕВЫЕ МОМЕНТЫ (1)

- Обеспечение кибернетической устойчивости - **непрерывный процесс** (цикл), в который вовлечены все, от клиентов банка, рядовых сотрудников и до топ-менеджеров;
- Ответственность за киберустойчивость д.брать на себя руководители (КУ перестала быть проблемой служб ИБ); **В частном секторе лица, управляющие бизнесом несут ответственность за непрерывность его ведения;**
- Достижение более высокого уровня КУ требует более глубокого анализа скрытых рисков;
- **Проектирование системы снизу вверх**. Архитектура системы должна быть адаптивной. Целесообразно использование специализированных средств реагирования, обеспечивающих план «Б»;
- Требуется **отечественная методическая база** для оценки уровня киберустойчивости и реализации мер по ее обеспечению;

КЛЮЧЕВЫЕ МОМЕНТЫ (2)

- КУ должна рассматриваться как неотъемлемый компонент получения выгоды, а не как способ предотвращения рисков, и нейтрализации последствий атак;
- Ключевая для успеха плана «Б» задача - оперативное, доверенное взаимодействие с другими участниками: регуляторами, клиентами, партнерами;
- Достоверная, своевременная, практически применимая информация о киберугрозах основной фактор, обеспечивающий возможность быстрого реагирования и восстановления;

КЛЮЧЕВЫЕ МОМЕНТЫ (3)

С акцентом на смежников-поставщиков-разработчиков

- **Использование аутсорсинга** услуг для оптимизации затрат при обеспечении КУ.

(Заказчику нужен долговременный сервис, в том числе и адаптация продукта под конкретные особенности и потребности заказчика, а не разовая закупка).

- **Разработка и проектирование критических систем** д. осуществляться таким образом, чтобы отказы таких систем происходили «как можно более предсказуемо и плавно». (Отчет американского центра по определению новых подходов к безопасности, 2014г.); Резервирование, оценка времени наработки на отказ, критичность к внешним воздействиям (сеть питания, каналы связи…..)

- **Использование безопасных стандартов программирования/кодирования** во время разработки, обновления и сопровождения ПО, а также во время его инспектирования и оценки. (Сегодня это не только хорошая практика, это требование).

- **Обеспечение киберустойчивости поставщика услуг, прежде всего критичных для заказчика.** (например, техническое обслуживание/поддержка СКЗИ, обслуживание центров управления, в т.ч. ключевой информацией.


infotecs
Спасибо!