Обеспечение киберустойчивости финансово-кредитной организации при взаимодействии с потребителями услуг.

Проблемные вопросы, требования и решения.

Панов С.Б.

ЭЛВИС-ПЛЮС

ПОЧЕМУ ТАКОЕ ВНИМАНИЕ КИБЕРПРОСТРАНСТВУ?

- информпространство строилось при приоритете юзабилити;
- число пользователей интернета ~ 2,5 млрд.;
- количество абонентов мобильной связи > 6 млрд.;
- переход в цифровую среду (прогноз по банкам на 10 лет): 90%;
- необходимо взаимодействовать с потребителем услуг –> невозможность построения «закрытой системы»
- 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*
- 48 % и 59 % отметили увеличение внимания к вопросам безопасности и рост инвестиций в этой сфере под влиянием программ по цифровой трансформации бизнеса. *PwC*

ТРЕБОВАНИЯ К УСТОЙЧИВОСТИ КИБЕРНЕТИЧЕСКОЙ СИСТЕМЫ

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

«Содержание обеспечения кибернетической безопасности может существенно отличаться в зависимости от назначения системы управления, специфики управляемого объекта, условий внешней среды, состава и состояния сил и средств управления, а также от порядка управления»

СПЕЦИФИКА ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Финансовая устойчивость коммерческого банка это способность в любой момент времени

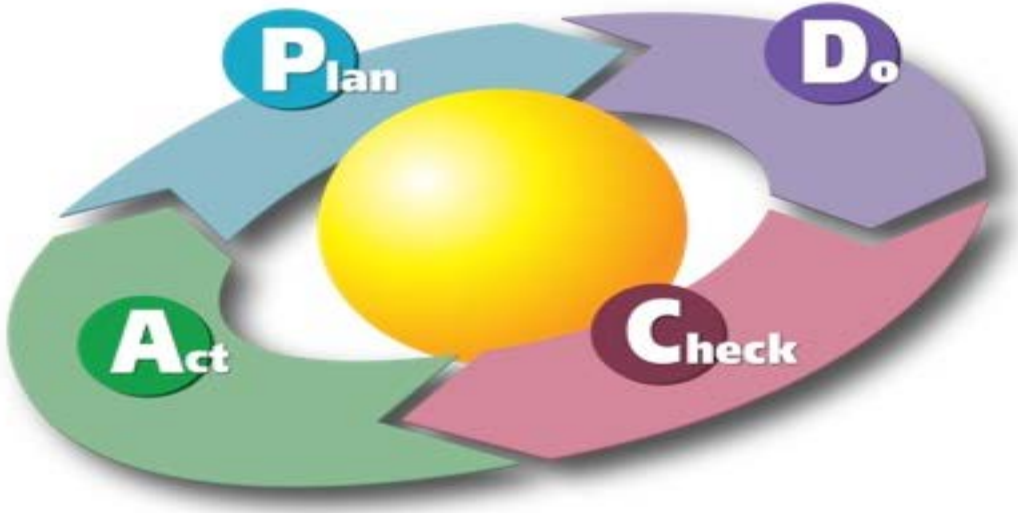
- Сохранять свои основные параметры деятельности (прибыль, капитал);
- Выполнять основные функции
  - аккумулирования денежных средств клиентов;
  - размещения их в кредиты и прочие активы;
- Выполнять обязательства по расчетам клиентов.

«Цель системы кибернетической устойчивости кредитной организации – обеспечить финансовую устойчивость в условиях негативных факторов кибернетических атак»

CPMI-IOSCO – Guidance on cyber resilience for financial market infrastructures – June 2016

Классическая методология менеджмента ИБ

1. Планирование (**P**lan)
2. Выполнение (**D**o)
3. Проверка (**C**heck)
4. Воздействие (**A**ct)



РЕАЛИЗУЕМА ЛИ «НЕПРОБИВАЕМАЯ» СИСТЕМА КБ?

- 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 кредитную организацию.

Пришло осознание - успешные кибератаки неизбежны.

Нужны другие подходы и методики, нужен план «Б»!

Методология адаптивной безопасности от Gartner

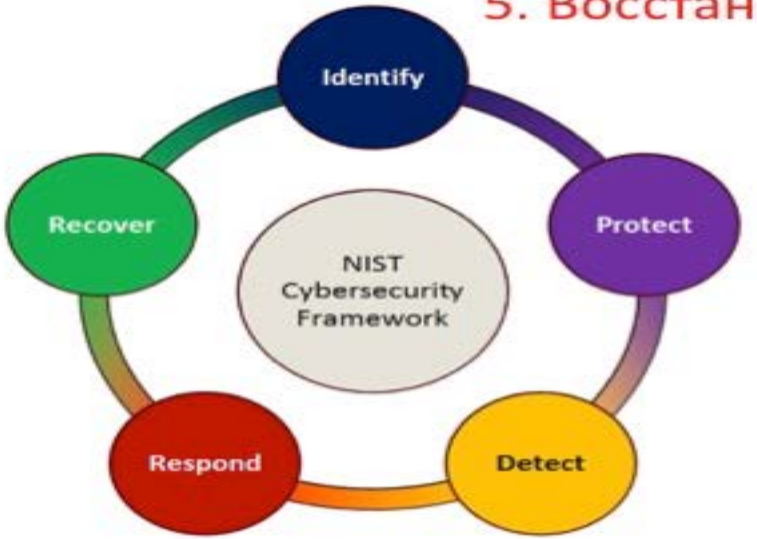
1. Прогнозирование (**Predict**)
2. Предотвращение (**Prevent**)
3. Обнаружение (**Detect**)
4. Реакция (**Respond**)

The Adaptive Security Architecture

Gartner

Методология кибербезопасности от NIST

1. Идентификация (**Identify**)
2. Защита (**Protect**)
3. Обнаружение (**Detect**)
4. Реагирование (**A**ct)
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 (**Act**)

- 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 «Б»

- ПРОГНОЗИРОВАТЬ;
- ПРЕДОТВРАЩАТЬ…

А если
не получилось?

На этот случай у меня есть…

ЧТО ЗНАЧИТ НАЛИЧИЕ ПЛАНА «Б»

1. Наличие соответствующих руководств и инструкций, обучение, подготовка персонала, проведение киберучений в организации по необходимым действиям в случае успешной кибератаки.
2. Развернутая техническая инфраструктура, адаптируемая, обеспечивающая выполнение критичных операций в условиях успешной кибератаки и последующее восстановление функционирования.

РЕГЛАМЕНТ ДЕЙСТВИЙ (ОРГ. СОСТАВЛЯЮЩАЯ) I

СУЩЕСТВУЮЩАЯ НОРМАТИВНАЯ БАЗА БР и АРБ ДЛЯ РАЗРАБОТКИ РЕГЛАМЕНТА ОБЕСПЕЧЕНИЯ ПЛАНА «Б» КИБЕРУСТОЙЧИВОСТИ:

- ПРИЛОЖЕНИЕ 5 Положения об организации внутреннего контроля в кредитных организациях и банковских группах
- РАЗДЕЛ 8.11 стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2014.
- Стандарт Программа управления непрерывностью деятельности кредитных организаций банковской системы Российской Федерации.

РЕГЛАМЕНТ ДЕЙСТВИЙ (ОРГ. СОСТАВЛЯЮЩАЯ) II

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*

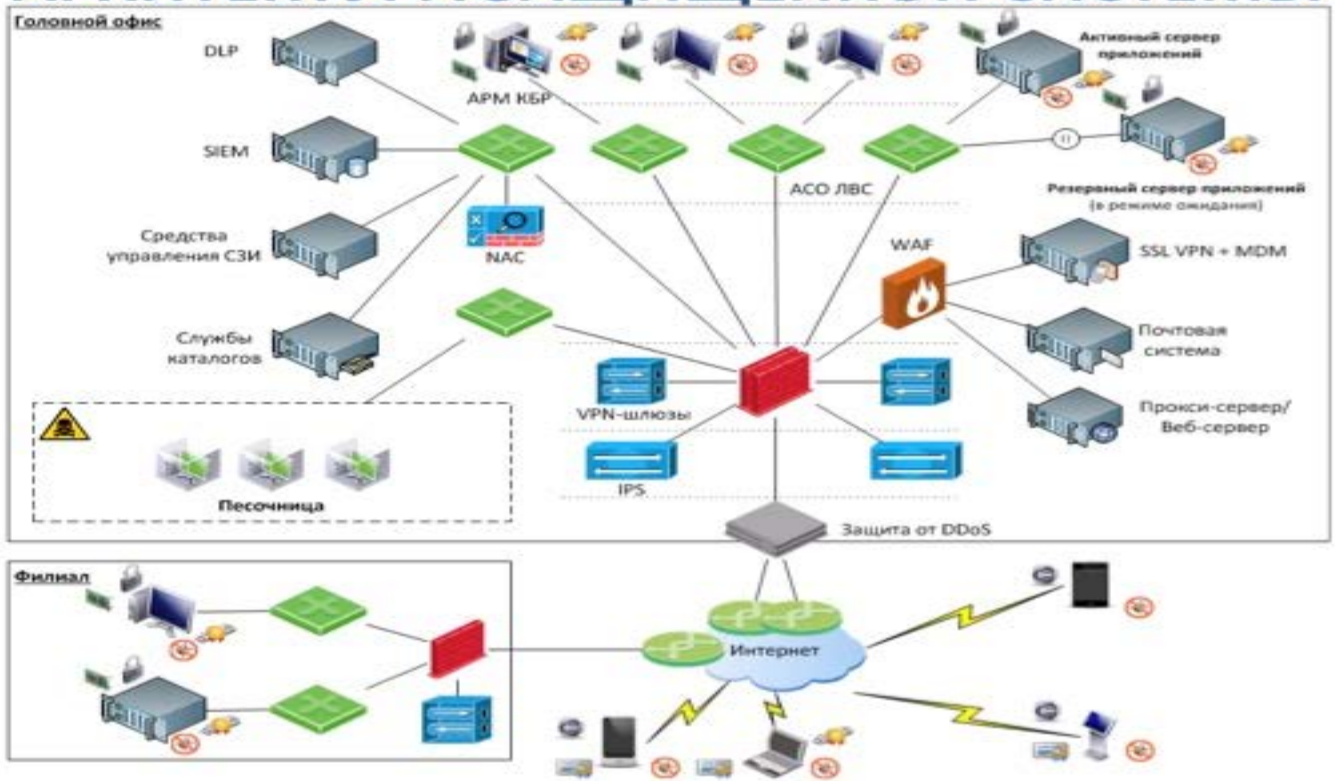
Частные руководства FFIEC, Federal Reserve Banks и т.д.

Руководство пользователей SWIFT.

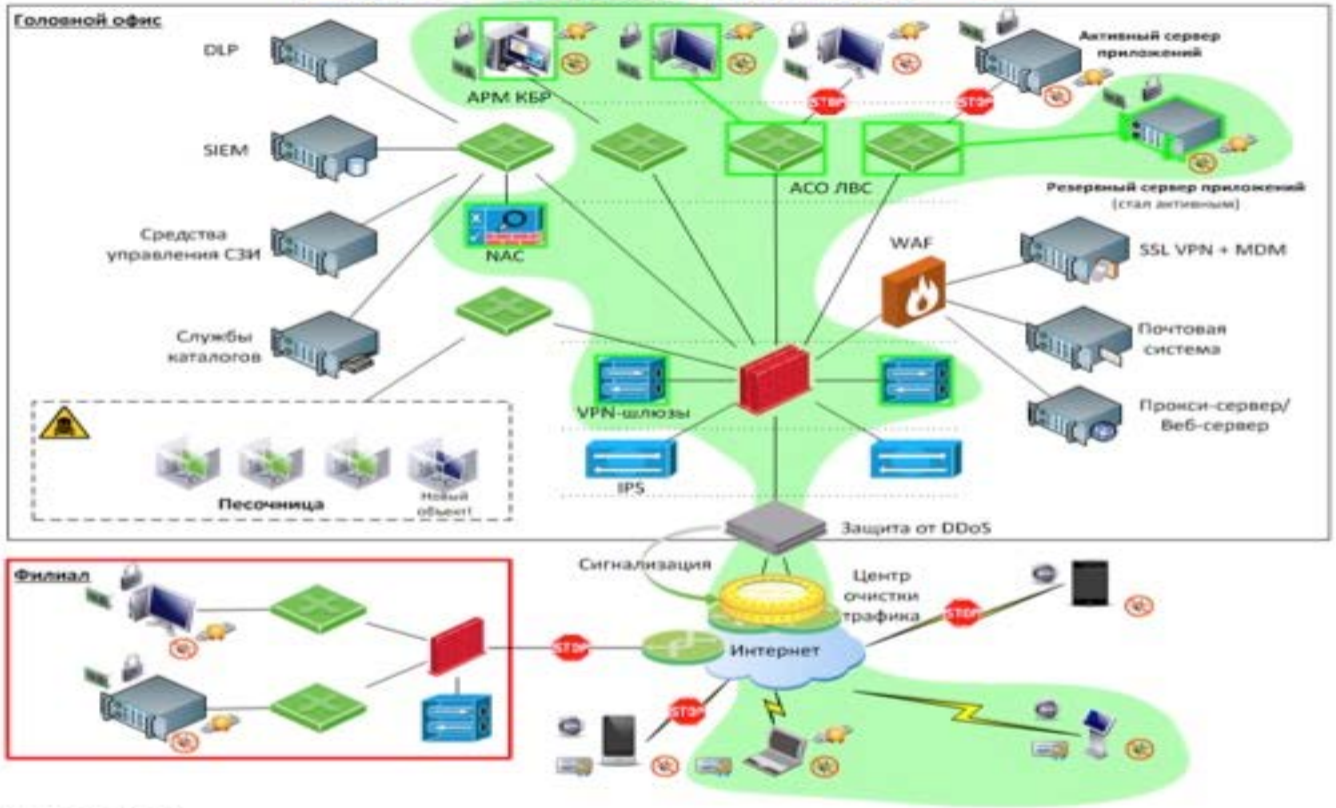
ТЕХНИЧЕСКАЯ ИНФРАСТРУКТУРА ПЛАНА «Б»

1. В рамках создания классических систем обеспечения информационной безопасности решаются задачи
   - ПРОГНОЗИРОВАНИЕ
   - ДЕТЕКТИРОВАНИЕ
   - ПРЕДОТВРАЩЕНИЕ
2. Акценты при реализации плана «Б»
   - ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ
   - ВОССТАНОВЛЕНИЕ

АРХИТЕКТУРА ЗАЩИЩЕННОЙ СИСТЕМЫ



РЕАГИРОВАНИЕ, ПЛАН «Б»



ПРОЕКТИРОВАНИЕ СНИЗУ ВВЕРХ

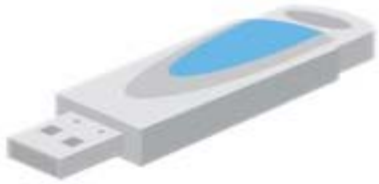
Общий пример – подход Trusted Computing Group

СТРОГАЯ АУТЕНТИФИКАЦИЯ КРИТИЧНЫХ СУБЪЕКТОВ И ОБЪЕКТОВ

Документ *CPMI-IOSCO, «Guidance on cyber resilience for financial market infrastructures»* прямо предписывает при управлении доступом использовать строгую аутентификацию.

ГОСТ Р ИСО/МЭК 9594-8-98

Строгая аутентификация - аутентификация, осуществляемая удостоверениями личности, полученными криптографическим способом.



БЕЗОПАСНОЕ КОДИРОВАНИЕ

МИНИМИЗАЦИЯ ВРЕМЕНИ И ЭФФЕКТИВНОСТЬ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

- Консолидация событий ИТ и ИБ в SIEM-системе.
- Проработка и поддержание в актуальном состоянии правил корреляции SIEM-системы, аналитическая и экспертная поддержка.
- Централизация и автоматизация управления СЗИ, инфраструктурой, конфигурациями, изменениями.
- Консолидация управления безопасностью и мониторинга в одном Центре, SOC

СПЕЦИАЛИЗИРОВАННЫЕ СРЕДСТВА РЕАГИРОВАНИЯ

Пример - Endpoint Detect & Respond (EDR)

- Выявление инцидентов ИБ в момент их возникновения на рабочем месте
  - Нарушение политики ИБ и подозрительная/вредоносная активность
  - Выявление известных угроз
  - Несанкционированное внесение изменений
  - Ретроспективный анализ накопленной информации
  - Динамический анализ потенциально опасных объектов с рабочих мест и выделенной «песочнице»
- Локализация инцидента в пределах масштаба на момент обнаружения
  - Предотвращение распространения угрозы средствами сторонних решений ИБ (например, антивирус/HIPS/DLP/HostFW)
  - Карантинизация рабочего места и объектов
  - Отключение прав и привилегий скомпрометированных аккаунтов
- Предоставление механизмов реагирования на уровне рабочих мест подверженных атаке
  - Откат до прежнего состояния (roll back) и восстановление (repair)
  - Удаление объектов, записей в реестре и т.д.
  - Блокирование процессов и несанкционированных активностей
- Поддержка проведения централизованных расследований инцидентов
  - Централизованный сбор необходимой информации с рабочих мест (дамп памяти и т.п.)
  - Централизованный «опрос» рабочих мест на предмет IOC или статическим скриптом
  - Хранение необходимой информации для ретроспективного анализа

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, регуляторов при подготовке и реализации планов “Б”;
- Для безопасной цифровизации бизнеса и услуг нужен кибер-просвещенный потребитель.

КЛЮЧЕВЫЕ МОМЕНТЫ

- Акцент на реагировании и восстановлении;
- Обеспечение кибернетической устойчивости - непрерывный процесс (цикл), в который вовлечены все, от клиентов банка, рядовых сотрудников и до топ-менеджеров;
- Проектирование системы снизу вверх. Архитектура системы должна быть адаптивной. Целесообразно использование специализированных средств реагирования, для поддержки плана «Б»;
- Разработка в рамках ТК отечественной методической базы для оценки уровня киберустойчивости и реализации мер по ее обеспечению;
- Ключевая для успеха плана «Б» задача - оперативное, доверенное взаимодействие с другими участниками финансового рынка: регуляторами, клиентами, партнерами;
- Использование аутсорсинга услуг для оптимизации затрат при обеспечении КУ. *PwC: Аутсорсинг облачных технологий защиты информации, переход на открытое программное обеспечение, безопасность корпоративной цифровой архитектуры и защита «интернета вещей» – ключевые технологические тренды кибербезопасности на 2017 год.*

Ваши вопросы?

ФИО докладчика