ГАЗИНФОРМСЕРВИС

Применение систем управления непрерывностью деятельности в условиях кибератак

Ведущий инженер ООО «Газинформсервис»
Черников Иван Васильевич

Магнитогорск, февраль 2016 г.

План доклада

- ✓Кибератаки и непрерывность бизнеса
- ✓Система управления непрерывностью деятельности
- ✓Автоматизация системы управления непрерывностью деятельности

Кибератаки и непрерывность бизнеса

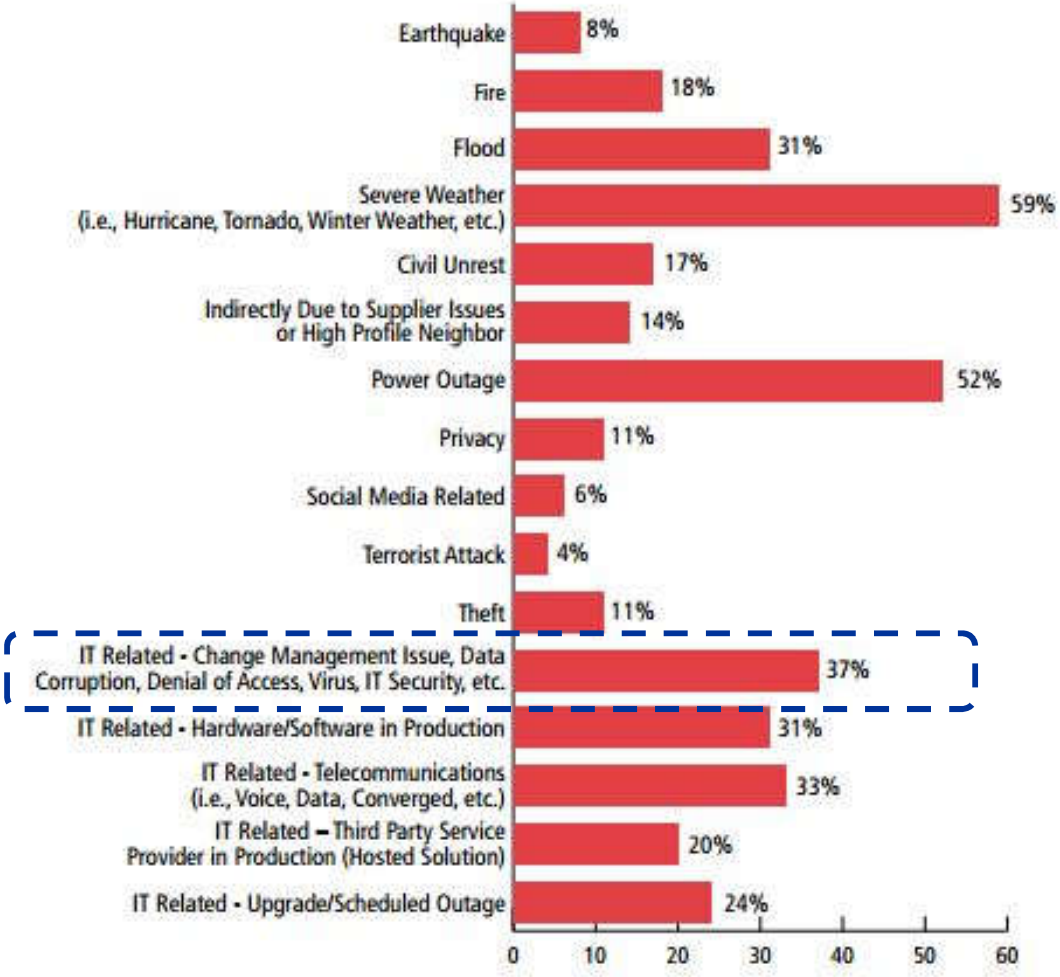
Результаты опроса The Business Continuity Institute
на тему главных угроз для ведения бизнеса

Threat	2012	2013	2014	2015
Cyber Attack	24%	25%	34%	43%
Unplanned IT & Telecoms Outage	30%	28%	31%	34%
Data Breach	28%	26%	29%	32%
Interruption to Utility Supply	18%	15%	18%	18%
Supply Chain Disruption	14%	10%	9%	13%
Security Incident	N/A	12%	14%	12%
Adverse Weather	19%	14%	18%	12%
Human Illness	7%	6%	10%	11%
Act of Terrorism	13%	10%	11%	11%
Fire	16%	11%	14%	10%

* – данные из отчета «Horizon Scan 2015 published by the Business Continuity Institute in association with the BSI»

Кибератаки и непрерывность бизнеса

Причины, по которым организации за последний год активировали планы ОНиВД

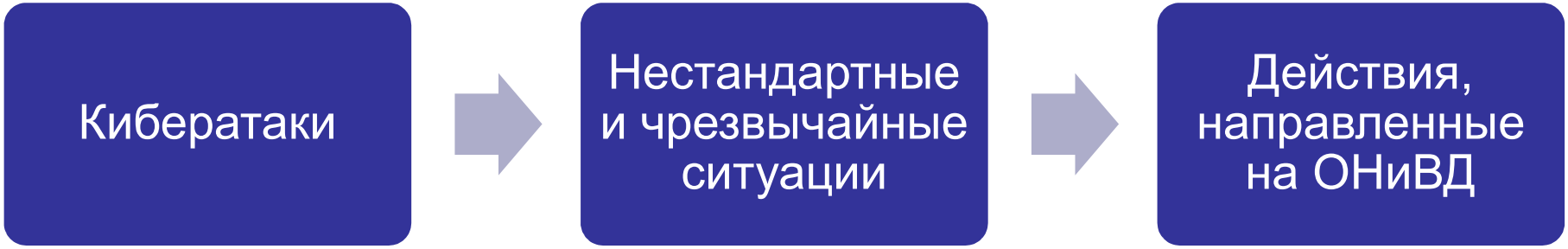


* – данные из «The 2013-2014 Continuity Insights and KPMG LLP Global Business Continuity Management Program Benchmarking Study»

Кибератаки и непрерывность бизнеса

Слайд с последствиями от простоев в банках

Система управления непрерывностью деятельности



Система управления непрерывностью деятельности

Основания для построения системы УНД в КФУ (пример)

- Положение Банка России от 16.12.03 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»
- Приказ ФСФР России от 25.06.13 № 13-53/пз-н
- СТО БР ИББС-1.0-2014 (8.11)
- ISO/IEC 27001:2013 (A.17)
- Положения стандарта PCI-DSS, Базельского комитета

Система управления непрерывностью деятельности

Основания для построения системы УНД в КФУ (пример)

X5 RETAIL GROUP

КОДЕКС ВЗАИМОДЕЙСТВИЯ

С БИЗНЕС-ПАРТНЕРАМИ

сотрудников и/или представителей, работающих на объектах Компании, а также обеспечивать их безопасность и надлежащие условия работы.

2.3.5. Прозрачность и аккуратность взаиморасчетов

Взаиморасчеты должны соответствовать условиям договора и реально поставленным товарам/услугам. Стороны не должны злоупотреблять своими правами. Взаиморасчеты и обмен отчетной документацией по договорам должны производиться аккуратно и с соблюдением согласованных сроков.

2.3.6. Надлежащее исполнение обязательств по договору

Мы настроены на поиск эффективных решений и развитие взаимовыгодного сотрудничества.

Мы ожидаем, что обязательства будут исполняться надлежащим образом. Мы ожидаем, что любые изменения принятых на себя обязательств будут являться результатом соответствующих переговоров.

Мы ожидаем, что Партнеры самостоятельно производят товары/услуги, распространением которых занимаются, либо имеют прямые контракты с производителями таких товаров и услуг, так как мы заинтересованы в построении эффективной и качественной цепочки поставок и удовлетворенности потребителей.

Если Партнер нанимает субподрядчика для исполнения обязательств перед Компанией (поставка товаров/оказание услуг), он должен обеспечить соблюдение субподрядчиком требований настоящего Кодекса.

2.3.7. Непрерывность бизнеса и кризисное управление

Компания ожидает, что Партнеры имеют адекватные процедуры, обеспечивающие непрерывность бизнес-процессов и позволяющие в случае технологических сбоев в кратчайший срок возобновлять предоставление продукции/услуг.

Система управления непрерывностью деятельности

Требования к системе УНД (пример)

Серия ISO 22300

- ISO 22301:2012 Societal security – Business continuity management systems – Requirements
- ISO 22313:2012 Societal security – Business continuity management systems – Guidance
- ISO/TS 22317:2015 Societal security – Business continuity management systems -- Guidelines for business impact analysis

ГОСТ Р 53647 «Менеджмент непрерывности бизнеса»

Стандарт управления непрерывностью деятельности организаций банковской системы РФ (АРБ)

Disaster Recovery Institute International Professional Practices

Система управления непрерывностью деятельности

Проблемы внедрения системы УНД

Число объектов и субъектов	• Структурирование • Контроль выполнения
Значительная неопределенность	• Формализация процесса • Степень охвата рисков
Взаимосвязь с другими видами деятельности	• Оперативный обмен • Дублирование данных

Система управления непрерывностью деятельности

Значительное число субъектов и объектов

Бизнес-процессы

Ресурсы

Требования регуляторов

Политика ОНиВД

Роли участников СУНД

Аудиты

Планы ОНиВД

Планы АВ

Сценарии

Задачи

Уведомления

Тесты планов

Несоответствия

Банковские риски

Риски нарушения НД

Анализ влияния на бизнес

Целевое время восстановления

Целевая точка восстановления

Максимально допустимое время простоя

Модули плана ОНиВД

Деревья обзвона

Инциденты ИБ

Чрезвычайные ситуации

Тревожный чемоданчик

Организационная структура/Работники

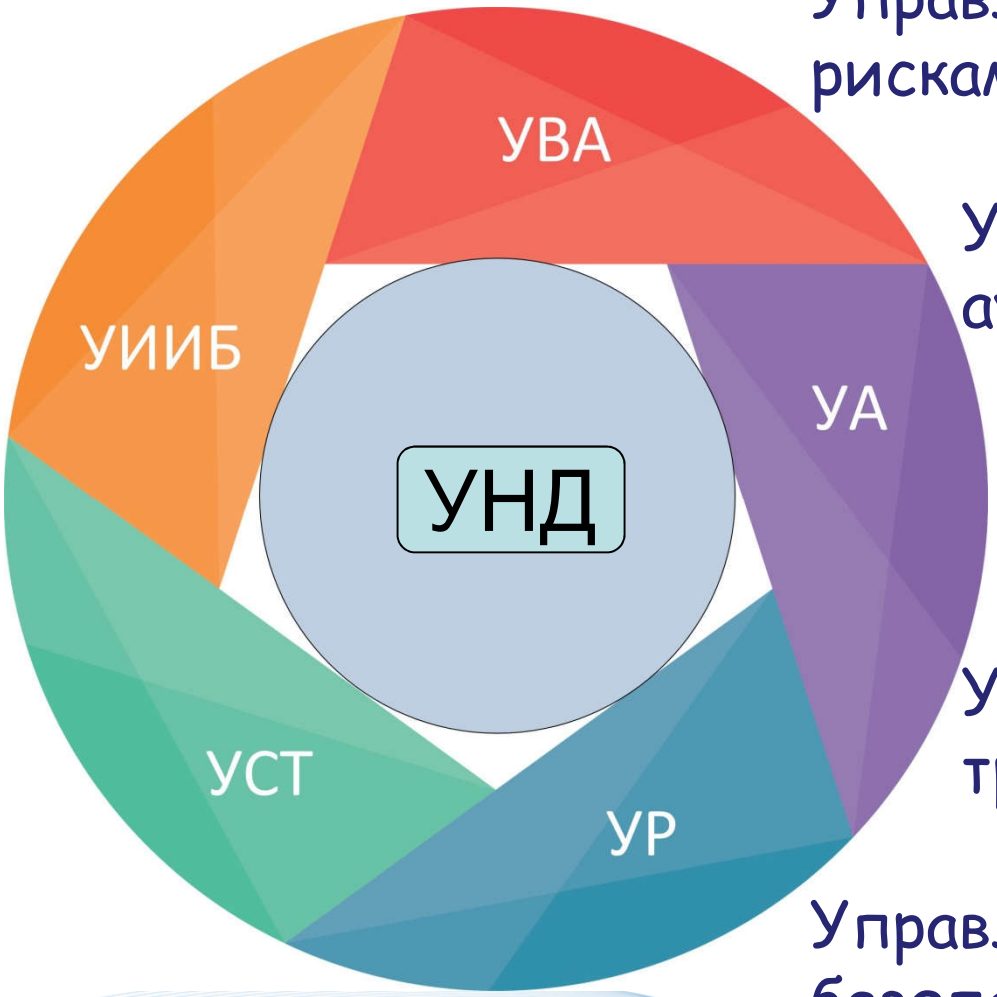
Система управления непрерывностью деятельности

Значительная неопределенность

* – на примере положений документа «Стандарт управления непрерывностью деятельности организаций банковской системы Российской Федерации» (Ассоциация российских банков)

Система управления непрерывностью деятельности

Взаимосвязь с другими видами деятельности



Управление банковскими рисками (УР)

Управление внутренними аудитами (УВА)

Управление ИТ-активами (ресурсами) (УА)

Управление соответствием требованиям (УСТ)

Управление инцидентами безопасности (УИИБ)

Автоматизация системы УНД

- Анализ рисков и влияния на бизнес
- Формирование и тестирование планов ОНиВД
- Управление чрезвычайными ситуациями
- Совершенствование системы УНД

Автоматизация системы УНД

✓Учет рисков нарушения непрерывности, их владельцев

✓Добавление связи рисков с потенциальными объектами воздействия, чрезвычайными ситуациями

✓Учет ресурсов, необходимых для восстановления деятельности (минимальный и обычный)

✓Проведение анализа влияния на бизнес (RTO, RPO)

Автоматизация системы УНД

✓Подготовка планов ОНиВД с учетом области действия (бизнес-процесс, риски, ресурсы, ИТ-активы)
✓Учет в планах рабочих процессов, деревьев обзвона, уведомлений, шаблонов для печати
✓Тестирование планов ОНиВД, осведомление
✓Учет несоответствий, выявленных в ходе тестирования, а также планов их устранения

Автоматизация системы УНД

Анализ рисков и влияния на бизнес

Формирование и тестирование планов ОНиВД

Управление чрезвычайными ситуациями

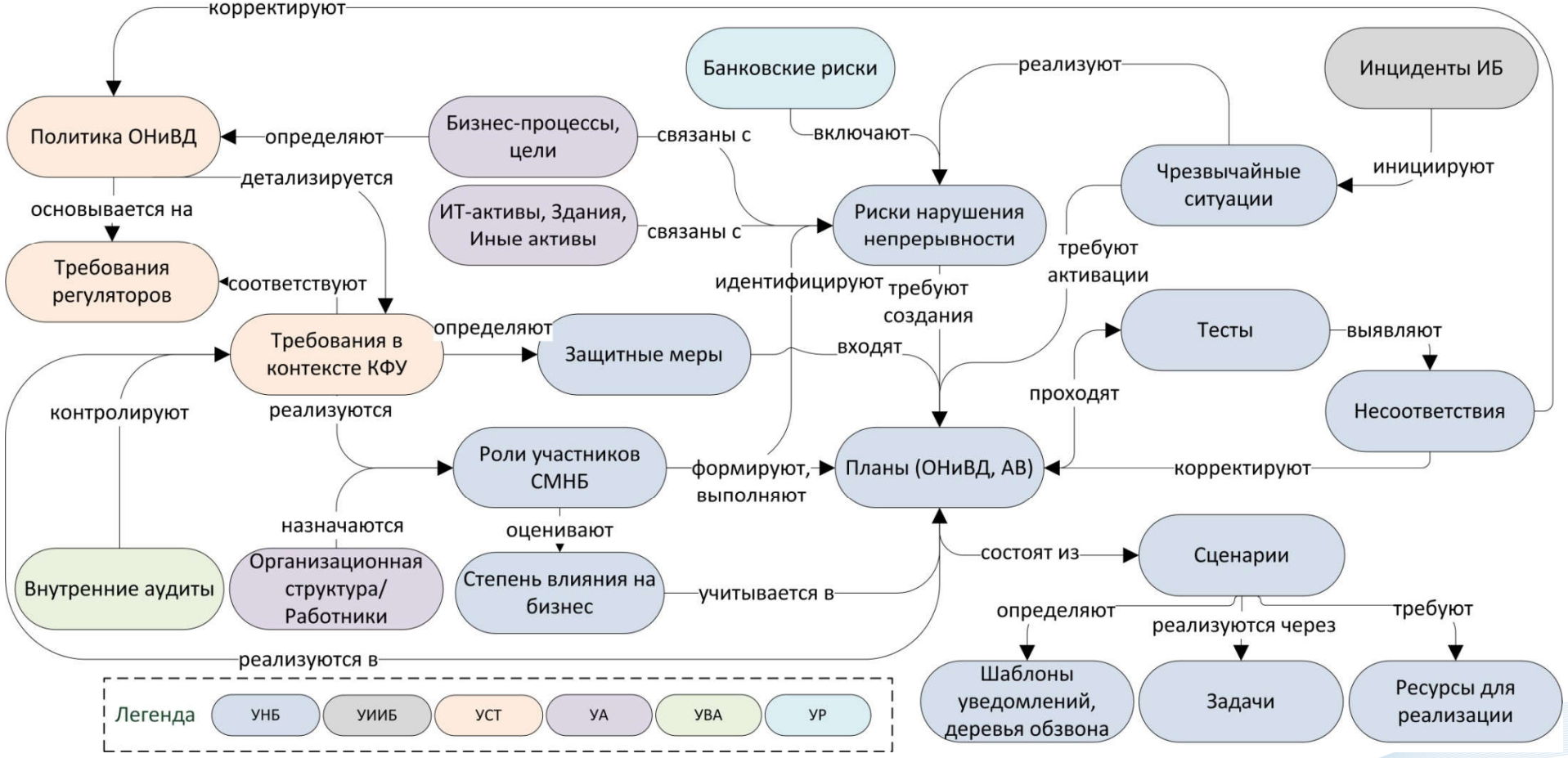
Совершенствование системы УНД

- ✓Регистрация и учет чрезвычайных ситуаций и вызвавших их инцидентов
- ✓Активация планов ОНиВД, деревьев обзвона
- ✓Отправка уведомлений по шаблонам
- ✓Учет времени выполнения, действий участников процесса УНД
- ✓Хранение всей истории по ЧС

Автоматизация системы УНД

- ✓Формирование показателей и метрик
- ✓Сбор данных о результатах измерений
- ✓Постановка и отслеживание задач для совершенствования системы УНД
- ✓Выполнение процедур внутреннего аудита

Автоматизация системы УНД



* – схема из BIS Journal – Информационная безопасность банков (01/2016)

Автоматизация системы УНД

- Внедрение системы УНД позволяет минимизировать последствия от нестандартных и чрезвычайных ситуаций (в том числе, вызванных кибератаками)
- Интеграция процесса УНД с другими видами управленческой деятельности позволяет получить максимальный эффект
- Автоматизация процесса УНД (например, на платформе GRC) позволяет оперативно осуществлять мониторинг системы УНД и принимать своевременные решения на каждом из этапов ее реализации

ГАЗИНФОРМСЕРВИС

Спасибо за внимание!

Ведущий инженер ООО «Газинформсервис»
Черников Иван Васильевич
ru.linkedin.com/in/IvanVChernikov

Магнитогорск, февраль 2016 г.