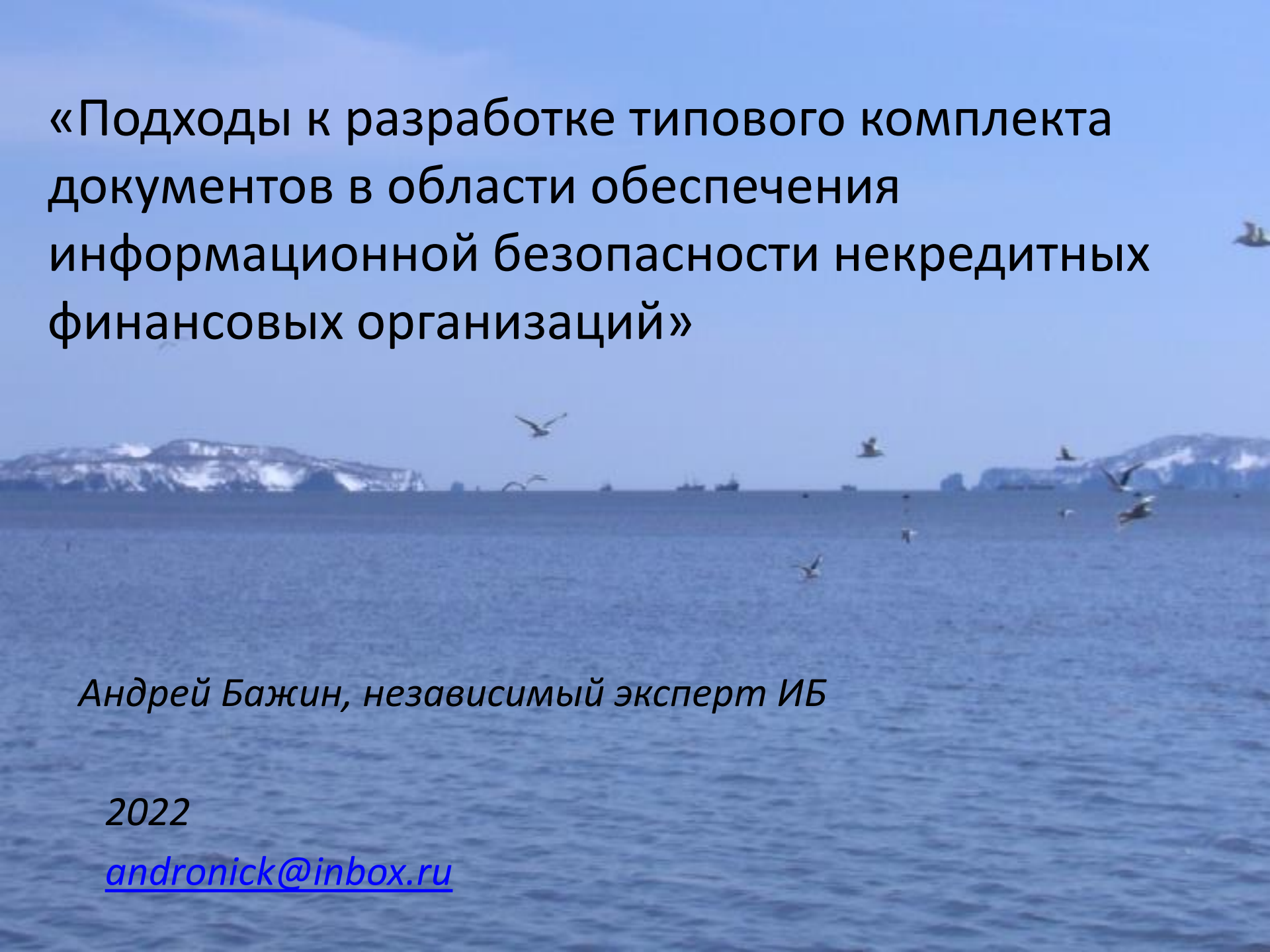
«Подходы к разработке типового комплекта документов в области обеспечения информационной безопасности некредитных финансовых организаций»



Андрей Бажин, независимый эксперт ИБ

2022

andronick@inbox.ru

Ключевые факторы успеха

1) привлечение руководства НКО

2) формирование внутренней компетенции по ИБ

3) в целом повышение уровня ИБ НКО, не только «бумажная» безопасность, но и практическая польза

4) выбор и утверждение целевого уровня ИБ, на основании которого будет делаться методология

5) выбор механизмов автоматизации разработки и поддержания в актуальном состоянии методологии ИТ и ИБ

6) формирование контрольной среды, в т.ч. отчетности и свидетельств реализации деятельности по ИБ

7) цикличность пересмотра методологии

8) обучение

Результаты опроса по ИБ НАУФОР

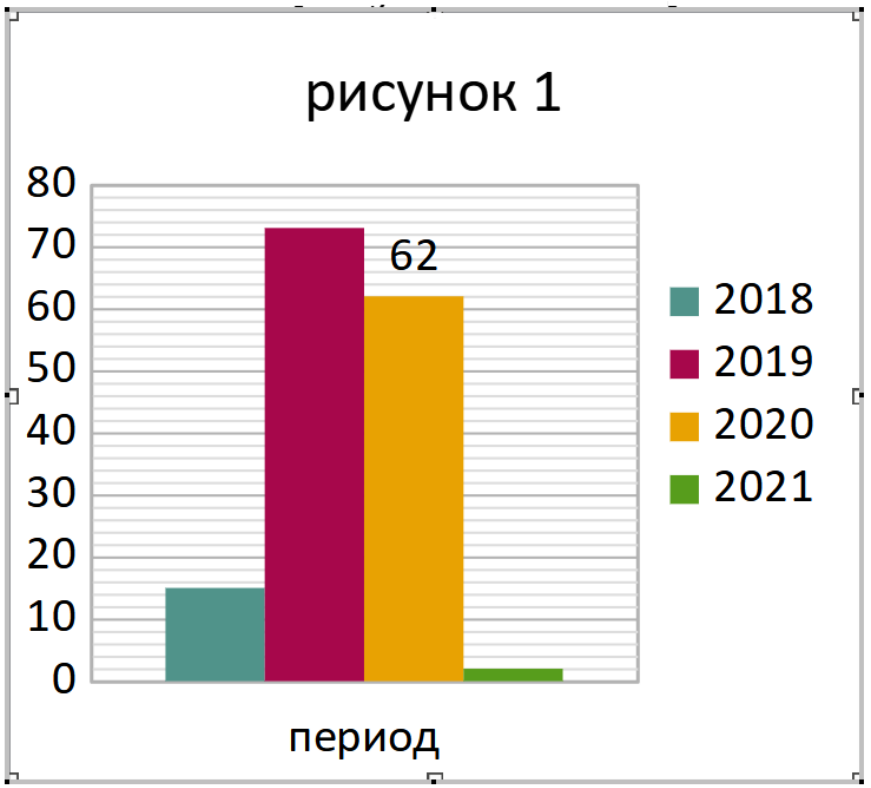
1) Мошенничество по завладению ценными бумагами без поручения клиента и(или) покушение на мошенничество: 1 попытка при помощи фишинга в 2021

2) Риски контрагентов, в части не предоставления услуг/сервисов: 1 событие в 2018 - 2020

3) Копирование информации о клиентах организации сотрудниками при увольнении: 1 событие в 2021

4) DDOS атака — 1 событие в 2021

5) Риски компаний клонов - мошенники выдают себя за реального брокера, размещают сайт с логотипом и/или названием компании (рисунок 1), 2



Результаты опроса по ИБ НАУФОР

Проблемы, отраженные участниками опроса:

1) недостаток сертифицированных средств защиты монобрендовых, что приводит к усложнению и удорожанию системы защиты

2) сложности с методологией ИБ, при том, что требуется перейти от функциональной модели ИБ к процессной

3) несовместимость некоторых средств защиты с существующим ИТ оборудованием, необходимость модернизации не только ИБ, но и ИТ инфраструктуры

4) увеличение расходов на информационную безопасность. Увеличение нагрузки на подразделения ИБ и ИТ.

Примеры рисков ИБ

1) атака на РЖД Белоруссии в январе 2022 года, совмещенная с [illegible] и политическими заявлениями
2) 28 декабря 2021 года [illegible] media [illegible] крупнейший [illegible] новостной [illegible] деятельность [illegible] приостановлена [illegible]»
3) 4 декабря 2021 года платформа BitMart по разным оценкам потеряла от 150 до 200 M$ в результате кибер атаки
4) американская платформа Robinhood была атакована 8 ноября 2021 года, похищены клиентские данные, в т.ч. почта и имена
5) 29 октября атака на национальный банк Пакистана, распределенная атака проникла во внутреннюю сеть банка, ATM и мобильные приложения
6) атака на сервисы wildberries
7) атаки на сервера арбитражных судов и размещение информации о спецоперации на Украине

Примеры рисков ИБ

1) атака на РЖД Белоруссии в январе 2022 года, совмещенная с [illegible] политическими заявлениями
2) 28 декабря 2021 года [illegible] крупнейший новостной [illegible] деятельность [illegible] »
3) 4 декабря 2021 года платформа BitMart по разным оценкам потеряла от 150 до 200 M$ в результате кибер атаки
4) 2021 года американская платформа Robinhood была атакована 8 ноября 2021 года, похищены клиентские данные, в т.ч. почта и имена
5) 29 октября атака на национальный банк Пакистана, распределенная атака затронула внутреннюю сеть банка, ATM и мобильные приложения
6) атака на сервисы wildberries
7) атаки на сервера арбитражных судов и размещение информации о спецоперации на Украине

Типовой план внедрения

1) Формируем рабочую группу:

- юристы, кадры, клиентский менеджмент, ИТ, ИБ, операционный директор, риски или внутренний контроль

2) Цели работы на первой стадии (мини устав проекта):

- определить, кто будет руководителем проекта (можно разделить по 3м основным направлениям: общие требования, ОУД4, требования к ИТ),
- как пойдет согласование
- кто будет отвечать за ИБ в НКО
- будет ли привлекаться внешний консультант и для чего или работы проводим своими силами
- оценить риск ИБ для компании посредством самооценки в т.ч. регуляторный
- стратегия по методологии: шаблоны или меняем существующие документы, KPI по согласованию
- сформировать предложения руководству о реализации проекта

Типовой план внедрения

1) формирование списка источников целевого уровня ИБ: 757- П и ГОСТ 57580, 779-П, 152-ФЗ и подзаконные акты, 149 -ФЗ, 63- ФЗ, 98 — ФЗ, ПКЗ2005 и т. д.,

2) в первую очередь акцент ЦБ будет на 757-П, то рекомендуется взять 757-П за основу формирования целевого уровня ИБ, соответственно: определить 5-7 процессов подпадающих под 757 — П,

3) явно определить, владельцев процессов

4) определить основные типы данных, которые участвуют в процессах и которые нужно защитить, п 1.1.:

- перс данные клиентов в т.ч. (контактные, паспортные и т.д.)
- финансовые данные (эл. сообщения)
- авторизационные данные (логин пароль и т.д.)
- ключевая информация (сертификаты, ключи и т. д.)
- журналы аудита

5) определить системы, которые подпадают под лицензируемую деятельность и в которых используются указанные выше данные

ии ИБ и должностные инструкции

6) сформировать план работ

7) зафиксировать указанные решения в приказах

Типовой план внедрения

Управление рисками ИБ:

За точку отсчета можно взять процесс управления операционным риском

Рекомендации по оценке рисков:

1) от угроз (вероятность) , от активов (стоимость), подход — количественный или качественный

2) разработать форму оценки рисков исходя из а) самих рисков: угроза, вероятность, последствия ($), контр меры ($) б) мер по мониторингу рисков, те как меняется величина риска во времени и каким способом реализуется мониторинг, например, риск шифровальщика, при наличии средств защиты, анализируются попытки проникновения эксплойтов, оцениваем частоту реализации данного риска

3) одни из самых важных рисков: редко случается, но последствия существенные, например потери от 10 мл, рублей , вероятность низкая, раз в 3-4 года может случиться, тк за 4 года вероятность вырастет

4) привлечь к процессу оценки рисков владельцев процессов

5) согласовать с руководством матрицу типов информации и владельцев, за клиентские данные отвечает — руководитель департамента клинского обслуживания, за данные сотрудников — HR директор и т. д., такие данные и такие системы могут быть подвержены таким — то рискам

Типовой план внедрения

Общие задачи:

1) самостоятельно или с привлечением консультанта провести оценку соответствия целевому уровню, создать некий инструмент, например, в XLS где все требования будут зафиксированы

2) сформировать детальный план, оценить бюджет и представить на рассмотрение руководству, обозначив приоритеты мер с точки зрения рисков, можно указать по каждой мере:

- возможные штрафы и последствия не реализации
- реальные риски, которые снимает та или иная мера, т. е. оценку потенциальных потерь
- требуемые ресурсы операционные и капитальные затраты

3) в минимальном объеме можно начать с обновления методологии: рекомендуется брать формулировки из законодательных актов и добавлять процедурные аспекты: описание функциональных ролей и зон ответственности, алгоритмов выполнения контрольных мер и форм отчетности (или журналов, которые могут быть подтверждением проведенных действий), т.к. при проверках ЦБ уделят внимание не только требованиям методического документа, но и доказательствам его реализации, хорошей практикой может быть разделение политик и процедур/регламентов

4) также рекомендуется пересмотреть положение по организации функции ИБ и должностные инструкции

Типовой плана внедрения

Завершающие активности:

1) Формирование внутренней отчетности или иных свидетельств реализации требований
2) ключевые индикаторы риска (количество инцидентов ИБ, количество выявленных хостов, не соответствующих требованиям ИБ, количество нарушений персоналом требований ИБ, количество критичных уязвимостей выявленных при сканировании / тесте на проникновение, просрочки ИТ по устранению уязвимостей и т.д.)
3) отчетность по ИБ: отчетность по инцидентам, отчетность по выполнению плана работ
4) заявки на доступ
5) журналы аудита
6) приказы о вводе средств защиты в эксплуатацию и т. д.
7) интегрировать процесс изменения в бизнес процессах и ИТ с ИБ, т. к. контрольная среда должна быть динамической