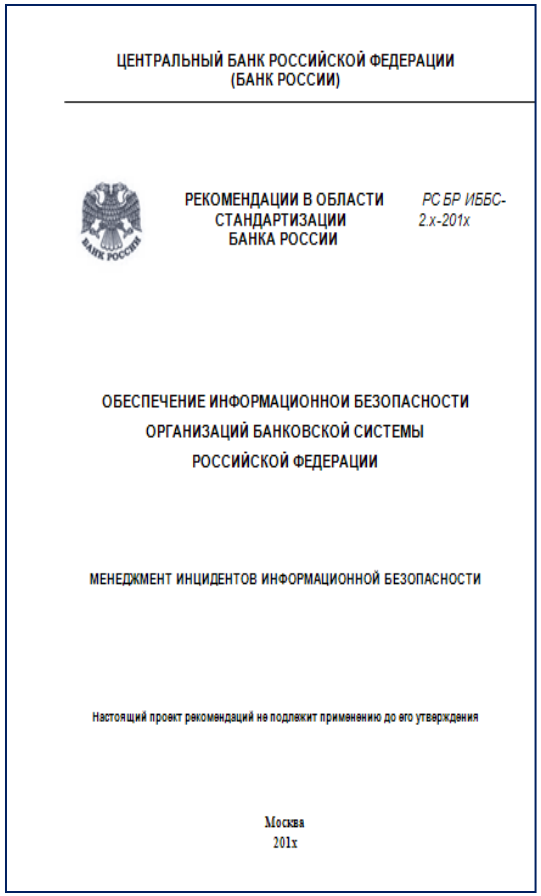
Вопросы применения рекомендаций по стандартизации Банка России по менеджменту инцидентов и предотвращению утечек информации

Велигура А.Н., CISA

Председатель комитета
по банковской безопасности
Ассоциации российских банков

Ассоциация Российских Банков

ПК1 ТК 122 ПОДГОТОВИЛ ПРОЕКТЫ РС БР ИББС



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

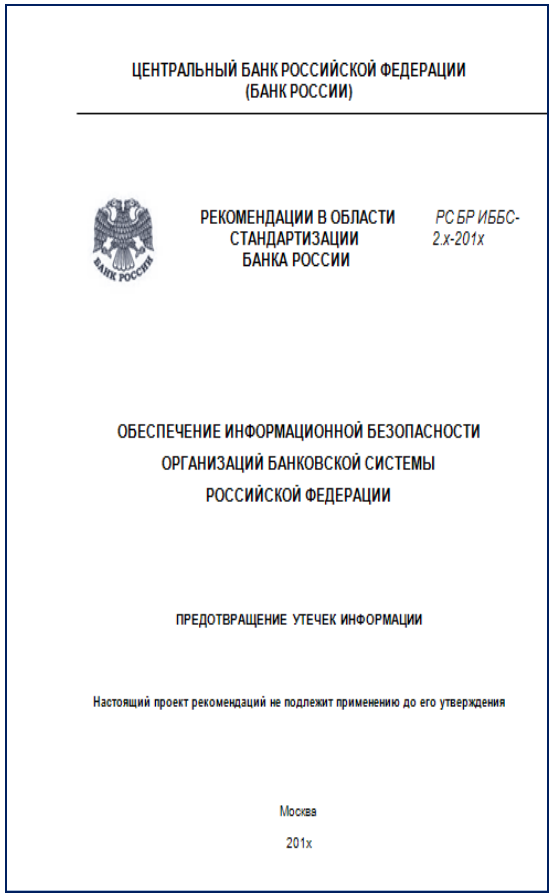
РС БР ИББС-2.х-201х

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящий проект рекомендаций не подлежит применению до его утверждения

Москва
201х



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

РС БР ИББС-2.х-201х

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

Настоящий проект рекомендаций не подлежит применению до его утверждения

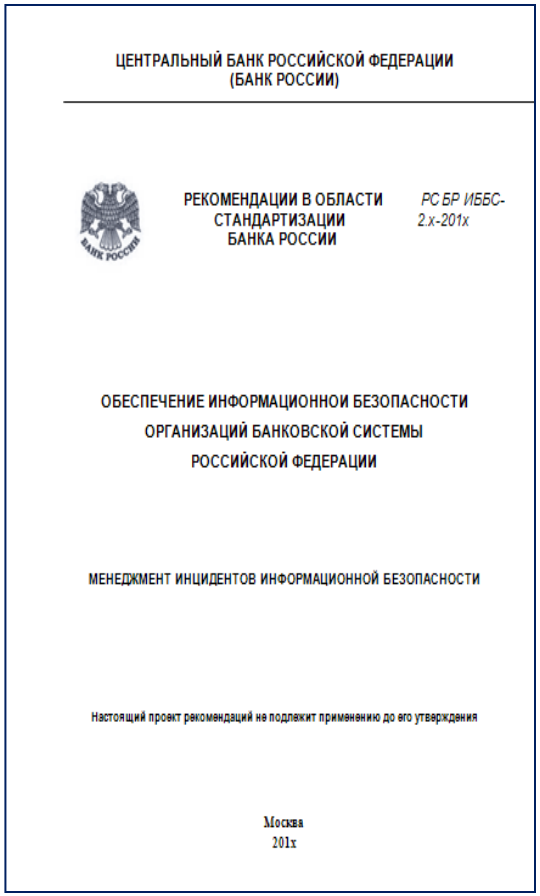
Москва
201х

Ассоциация Российских Банков

ОБЩИЙ ПОДХОД (в соответствии со СТО БР ИББС-1.0)

Для предотвращения утечек информации организации БС РФ рекомендуется реализовать ряд процессов, сгруппированных в виде циклической модели Деминга: “… - планирование — реализация — анализ — совершенствование—планирование — …”.

Для реализации, эксплуатации, контроля и поддержания на должном уровне менеджмента инцидентов ИБ организации БС РФ рекомендуется реализовать ряд процессов системы менеджмента инцидентов ИБ, сгруппированных в виде циклической модели Деминга: «…– планирование – реализация – анализ – совершенствование – планирование – …».



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

РС БР ИББС-2.х-201х

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящий проект рекомендаций не подлежит применению до его утверждения

Москва
201х

РС «МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ »

Эти процессы должны описывать

- стадию обнаружения, оповещения и оценки событий ИБ,
- стадию сбора и фиксации информации, относящейся к инциденту ИБ;
- стадию закрытия инцидента
- стадию анализа собранной информации и принятия управленческих решений

реагирование

С учетом ГОСТ Р ИСО/МЭК 18044, ISO 27035

РС «МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ »

Общий подход к выявлению ИИБ, конкретизирующий этот процесс по сравнению с известными стандартами, предполагает, что:

<u>определяются</u>

- перечень событий ИБ (возможных инцидентов)
- порядок их обнаружения
- порядок их оценки

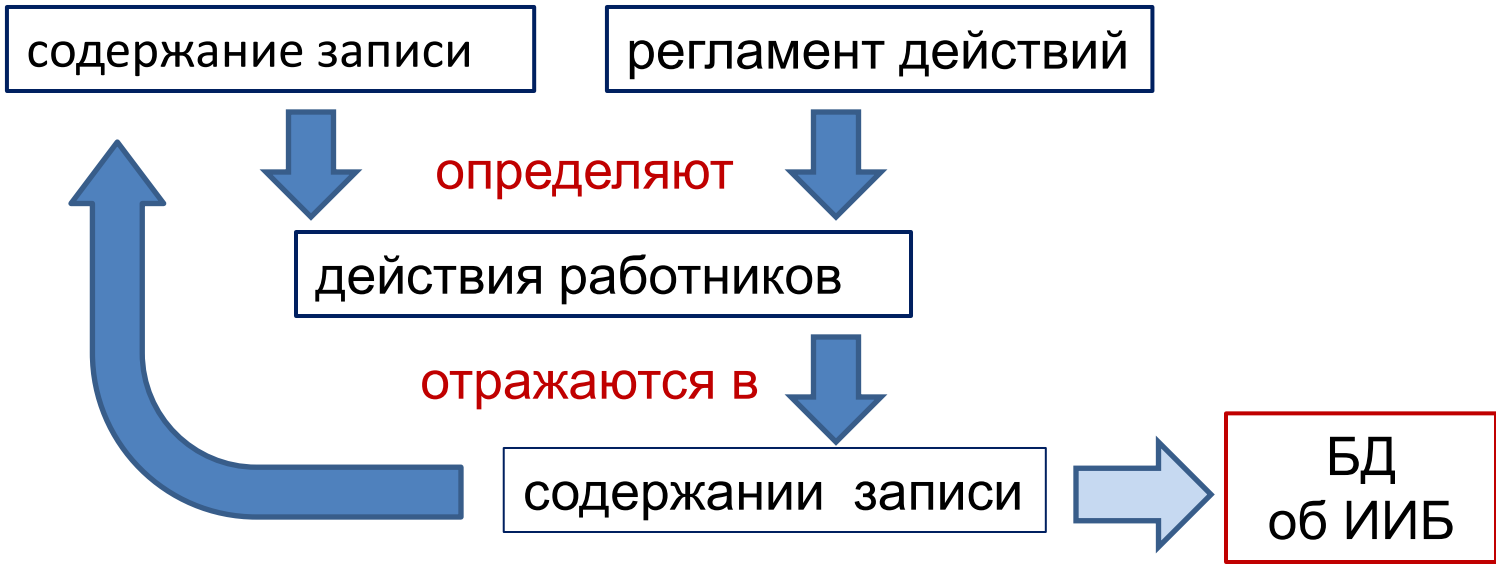
В Приложении 1 приведен примерный перечень типов событий ИБ

РС «МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ »

Общий принцип организации реагирования:

при выявлении инцидента создается запись об инциденте.

Далее :



РС «МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ »

Структура (формат и содержание полей) записи об инциденте определяется классификатором инцидентов ИБ.

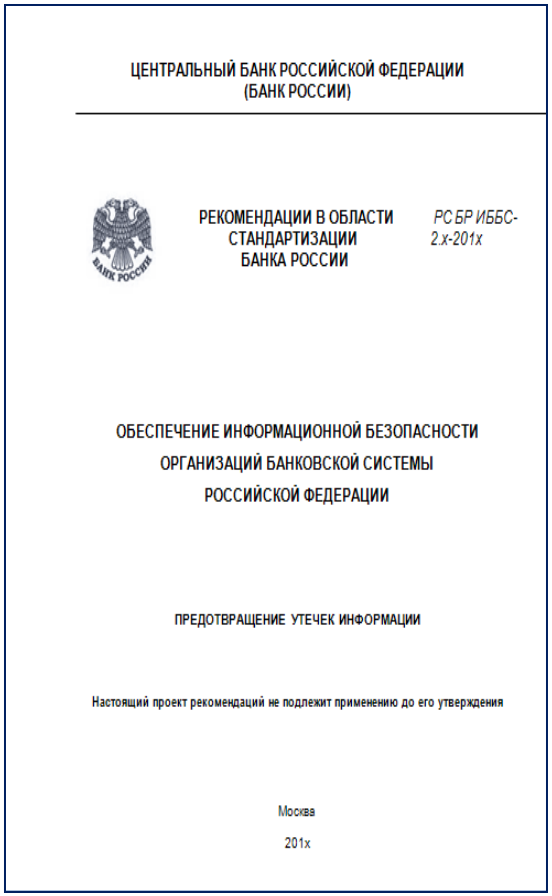
Примерный классификатор инцидентов ИБ приведен в Приложении 2 к РС.

РС «МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ »

Рекомендации к определению ролей процесса реагирования на инциденты ИБ даны применительно к ГРИИБ – группе реагирования на инциденты ИБ.

ГРИИБ – действующая на постоянной основе группа работников организации БС РФ, которая выполняет установленные в организации БС РФ процедуры реагирования на инциденты ИБ.

В РС не предполагается, что это структурное подразделение.



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

РС БР ИББС-2.х-201х

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

Настоящий проект рекомендаций не подлежит применению до его утверждения

Москва

201х

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

Утечка информации – инцидент информационной безопасности, состоящий в потере контроля над информацией, подлежащей защите, или в предоставлении несанкционированного доступа к этой информации, в том числе неопределенному кругу лиц, в результате действий или бездействия лица, имеющего легитимный доступ к данной информации.

Ассоциация Российских Банков

ОСОБЕННОСТИ ПРИМЕНЕНИЯ РЕКОМЕНДАЦИЙ

Детализация модели угроз:

- источники угрозы утечки информации – внутренние нарушители;
- уязвимости системы обеспечения ИБ, наличие которых влияет на возможность утечки
- способы реализации угрозы
- объекты информационной инфраструктуры, подвергающиеся воздействию при утечке

Ассоциация Российских Банков

ИСТОЧНИКИ УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ

1. Лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступа к АБС
2. Пользователи АБС, осуществляющие ограниченный доступ к ресурсам АБС с АРМ.
3. Пользователи АБС, осуществляющие ограниченный доступ к ресурсам АБС по сети.
4. Пользователи АБС с полномочиями администратора безопасности структурного подразделения защищаемой АБС.
5. Пользователи с полномочиями системного администратора АБС.
6. Пользователи с полномочиями администратора безопасности АБС.
7. Программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте.
8. Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АБС.

Ассоциация Российских Банков

УЯЗВИМОСТИ СОИБ, НАЛИЧИЕ КОТОРЫХ ВЛИЯЕТ НА ВОЗМОЖНОСТЬ УТЕЧКИ

1. Уязвимости, связанные с организацией обеспечения ИБ

- Отсутствие или невыполнение регламентов и требований по обеспечению ИБ,
- Отсутствие контроля выполнения регламентов и требований в области обеспечения ИБ,
- Отсутствие ресурсов или персонала, необходимых для эксплуатации или защиты от утечек информации
- Наличие возможности выноса средств обработки и/или носителей информации за пределы контролируемой зоны
- Размещение элементов информационной инфраструктуры вне контролируемой зоны, в местах доступных для неуполномоченных лиц, в непригодных или непредназначенных для этого помещениях
- Нахождение каналов связи, по которым передается защищаемая информация, вне пределов контролируемой зоны

2. Уязвимости, связанные с персоналом

- Неблагонадежность персонала, работающего с информацией, подлежащей защите от утечек
- Недостаточная квалификация персонала, работающего с информацией, подлежащей защите от утечек

3.Технические уязвимости

- Отсутствие или неэффективность мер защиты АБС
- Ошибки в системном и прикладном ПО
- Ошибки в настройках оборудования, ПО, СЗИ
- Наличие возможности использования персональных средств обработки информации (принадлежащих пользователю)
- Наличие корпоративных сервисов, обеспечивающих передачу и обмен защищаемой информацией
- Наличие корпоративных сервисов, обеспечивающих удаленный доступ к сервисам передачи и обмена защищаемой информацией
- Наличие доступа пользователей защищаемой информации к сети Интернет
- Наличие возможности самостоятельной установки ПО пользователями средств обработки защищаемой информации

Ассоциация Российских Банков

СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗЫ

1. Потеря, кража носителей информации и/или средства обработки информации
2. Передача информации неуполномоченным лицам внутри/вне организации БС РФ по каналам электронной почты, по телефонной связи, при личном контакте
3. Передача носителей информации неуполномоченным лицам внутри/вне организации БС РФ
4. Нелегитимная передача информации посредством интернет-сервисов, в том числе размещение информации на общедоступных ресурсах сети Интернет
5. Неправильная утилизация носителя информации и/или средства обработки информации
6. Передача информации посредством корпоративных ИТ-сервисов и/или предоставление доступа нелегитимным получателям
7. Нелегитимная передача информации посредством использования персональных ИТ-сервисов передачи информации
8. Несанкционированная фото/видео/аудио запись информации с дальнейшей обработкой и/или передачей
9. Конспектирование информации, запоминание информации
10. Разглашение информации

Ассоциация Российских Банков

СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗЫ

1. Потеря, кража носителей информации и/или средства обработки информации
2. Передача информации неуполномоченным лицам внутри/вне организации БС РФ по каналам электронной почты, по телефонной связи, при личном контакте
3. Передача носителей информации неуполномоченным лицам внутри/вне организации БС РФ
4. Нелегитимная передача информации посредством интернет-сервисов, в том числе размещение информации на общедоступных ресурсах сети Интернет
5. Неправильная утилизация носителя информации и/или средства обработки информации
6. Передача информации посредством корпоративных ИТ-сервисов и/или предоставление доступа нелегитимным получателям
7. Нелегитимная передача информации посредством использования персональных ИТ-сервисов передачи информации
8. Несанкционированная фото/видео/аудио запись информации с дальнейшей обработкой и/или передачей
9. Конспектирование информации, запоминание информации
10. Разглашение информации

Ассоциация Российских Банков

РЕАЛИЗАЦИЯ УГРОЗЫ

МОЖЕТ ВКЛЮЧАТЬ

- Отключение СЗИ
- Подключение к другим сетям передачи данных
- Изменение маршрутизации
- Маскирование информации

МОЖЕТ ИСПОЛЬЗОВАТЬ

- Корпоративные стационарные и/или мобильные средства обработки и/или хранения информации
- Корпоративные съемные носители информации
- Бумажные носители (твердые копии)
- Персональные стационарные средства обработки и/или хранения информации
- Персональные мобильные средства обработки информации (BYOD)
- Персональные съемные носители информации

РЕАЛИЗАЦИЯ УГРОЗЫ

МОЖЕТ ИСПОЛЬЗОВАТЬ ТАКИЕ СЕРВИСЫ, КАК

- Корпоративная электронная почта
- Сервисы мгновенных сообщений
- Удаленный доступ к рабочему столу
- Удаленный доступ к корпоративной электронной почте
- Корпоративный информационный портал
- Удаленный доступ к корпоративному информационному порталу
- Корпоративный файлообменный сервис
- Удаленный доступ к корпоративным специализированным информационным системам

Ассоциация Российских Банков

ОБЪЕКТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, ПОДВЕРГАЮЩИЕСЯ ВОЗДЕЙСТВИЮ ПРИ УТЕЧКЕ

Защищаемая информация

К числу информационных активов, подлежащих защите от утечек информации, рекомендуется отнести:

- информацию, подлежащую защите в соответствии с законодательством Российской Федерации и(или) в соответствии с внутренними нормативными документами организации БС РФ;
- информацию о руководстве организации БС РФ;
- информацию о сотрудниках организации БС РФ;
- информацию о деятельности организации БС РФ.

} за исключением открытой (общедоступной) информации

Спасибо за внимание!

Велигура Александр Николаевич

Председатель комитета
по банковской безопасности
Ассоциации российских банков

Председатель комитета
по безопасности
Национального платежного совета

Заместитель генерального директора
ООО Андэк Консалтинг

Москва, ул.Серпуховской Вал,19-8
Телефон:+7 (495) 984-60-40
E-mail: a.veligura@andekconsult.ru


АРБ
Ассоциация
Российских
Банков