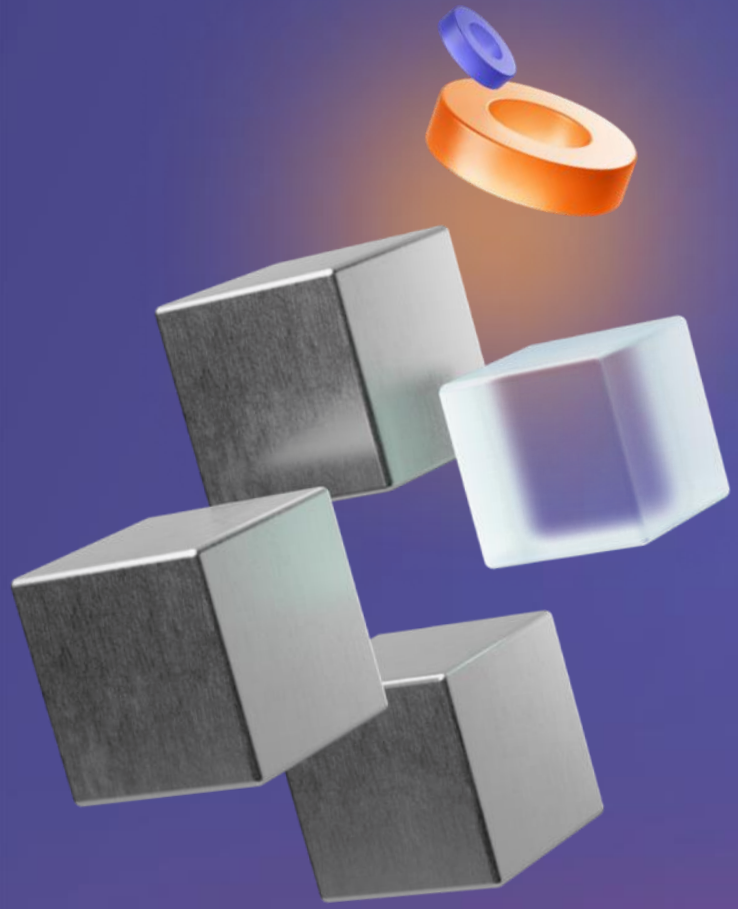


psbank.ru

Кадровое обеспечение команд управления ИБ на примере распределенной организационной структуры

Департамент информационной безопасности,
ПАО Промсвязьбанк

Шведов Сергей Владимирович

Заместитель директора департамента - директор по техническому сопровождению и технологической экспертизе

01

ПСБ – универсальный, системно значимый банк

ПСБ – универсальный, системно значимый банк с государственным участием

НАДЕЖНО

опорный банк для осуществления гособоронзаказа

СИСТЕМНО

банк с 25-летней историей, для бизнеса и людей

ЗНАЧИМО

включен в список стратегических предприятий России

Офисы во всех ФО

Собственная Банкоматная сеть

ПСБ – банк для бизнеса и людей

Филиалы банка: ЦФО, СЗФО, ЮФО, СКФО, УФО, СФО, ДФО, Крым, НС

Первым начал обслуживать клиентов в новых субъектах РФ[1]

Является **доверенным лицом** УЦ ФНС

Многие информационные системы, включая системы дистанционного банковского обслуживания **собственной разработки**

Участник системы **цифрового рубля**[2] Банка России

Банк является субъектом **КИИ**

[1] ЛНР, ДНР, Запорожская и Херсонские области, 2023 год
[2] Входит в пилотную группу банков, решение успешно встроено в мобильное приложение для Android

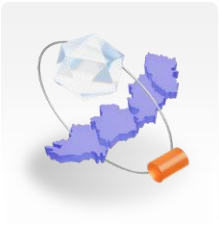
02

Направления деятельности подразделений информационной безопасности

Особенности банка влияющие на структуру подразделений информационной безопасности

Департамент информационной безопасности – отдельное **самостоятельное структурное подразделение** в банке

Основной состав **ДИБ** размещен в головном офисе в Москве



В каждом филиале (включая новые субъекты РФ[1]) присутствует отдел защиты информации, подчиняющиеся ДИБ ГО

В банке несколько УЦ, включая аккредитованный, сопровождает ДИБ

Более 1000 разработчиков и более 100 проектов разработки и внедрения ПО

Ресурсные ИТ центры: Москва, Санкт-Петербург, Самара, Ижевск, Ярославль

[1] Крым, Севастополь, ЛНР, ДНР, Запорожская и Херсонские области

Направления деятельности подразделений информационной безопасности

Функциональные обязанности сотрудников подразделений информационной безопасности

- Разработка нормативных документов и требований по ИБ
- Методологическая помощь структурным подразделениям
- Контроль выполнения внутренних и регуляторных требований ИБ
- Проектирование систем ИБ
- Проектирование подсистем ИБ и выработка требования ИБ для информационных систем
- Внедрение систем ИБ и подсистем ИБ в информационных системах
- Администрирование и сопровождение систем ИБ
- Автоматизация сбора и корреляции событий ИБ
- Аудит защищенности информационных систем
- Аудит защищенности сетевой инфраструктуры
- Разработка и внедрение стандартов настроек
- Контроль исполнения стандартов настроек
- Установка и настройка средств защиты в информационных системах
- Организация учета и распространения средств криптографической защиты
- Администрирование УЦ и HSM
- Анализ защищенности информационных систем
- Разработка эксплуатационной документации на средства обеспечения ИБ
- Анализ угроз информационной безопасности
- Организация и контроль процесса управления рисками ИБ
- Выявление, идентификация и оценка рисков
- Сбор и регистрация информации о выявленных рисках
- Мониторинг рисков информационной безопасности и контроль показателей уровня рисков ИБ
- Мониторинг, выявление и регистрация инцидентов ИБ
- Противодействие активности мошенников, несанкционированным списаниям денежных средств
- Реагирование на инциденты ИБ
- Расследование инцидентов ИБ
- Подготовка отчетов по инцидентам ИБ
- Проведение проверок по выполнениям требований ИБ
- Статический анализ кода ПО
- Анализ ПО и модулей ПО на НДВ
- Анализ заявок на создание и изменение информационных систем
- Анализ заявок на ролевой доступ
- Анализ заявок на сетевой доступ
- Анализ заявок на доступ ТУЗ и сервисов

Матрица полномочий

	Разработка нормативных документов и требований по ИБ	Методологическая помощь структурным подразделениям	Контроль выполнения внутренних и регуляторных требований ИБ	Проектирование систем ИБ	Проектирование подсистем ИБ и выработка требований ИБ для информационных систем	Внедрение систем ИБ и подсистем ИБ в информационных системах	Администрирование и сопровождение систем ИБ	Автоматизация сбора и корреляции событий ИБ	Аудит защищенности информационных систем	Аудит защищенности сетевой инфраструктуры	Разработка и внедрение стандартов настроек	Контроль исполнения стандартов настроек	Установка и настройка средств защиты в информационных системах	Организация учета и распределение средств криптографической защиты	Администрирование УЦ и HSM	Анализ защищенности информационных систем	Разработка эксплуатационной документации на средства обеспечения ИБ	Анализ угроз информационной безопасности	Организация и контроль процесса управления рисками ИБ	Выявление, идентификация и оценка рисков	Сбор и регистрация информации о выявленных рисках	Мониторинг рисков информационной безопасности и контроль показателей уровня рисков ИБ	Мониторинг, выявление и регистрация инцидентов ИБ	Противодействие активности мошенников, несанкционированным списаниям денежных средств	Реагирование на инциденты ИБ	Расследование инцидентов ИБ	Подготовка отчетов по инцидентам ИБ	Проведение проверок на выполнение требований ИБ	Статический анализ кода ПО	Анализ ПО и модулей ПО на НДВ	Анализ заявок на создание и изменение информационных систем	Анализ заявок на ролевой доступ	Анализ заявок на сетевой доступ	Анализ заявок на доступ ТУЗ и сервисов
Методолог	О и	и	О															О и К	О и К	и								и				и	и		
Эксперт по рискам ИБ	и	и	и						и	и								О и К	О и К	О и К	О и	О и К													
Администратор доступов		и		и	и	и	и											и		и	и		и		и								и	и	и
Аудитор (контролер) исполнения требований ИБ	и К	и	К	К	К	К		К	К	К		К		К	К	К		К	К	и	К		К	К	К	К	К	О и							
Администратор средств периметральной защиты				и	и		и	и				и	и				и	и		и	и				и	и								
Администратор средств защиты внутренних сетевых ресурсов				и	и		и	и				и	и				и	и		и	и				и	и								
Администратор средств защиты информационных систем				и	и	О и	и	и				и	и					и		и	и				и	и								
Администратор инфраструктуры и платформ обеспечения ИБ			и	и	и	О и	и	и					и				и	и		и														
Архитектор средств защиты сетевой инфраструктуры	и		и	О и	О и	О и		и			и							и	и													и		и	и
Архитектор средств защиты информационных систем	и		и	О и	О и	О и		и			и							и	и													и		и	и
Аудитор технологических процессов (технолог)			и	и	и	О и		и	и	и		и					и	и	и	и	и									и		и		и	и
Специалист по процессам безопасной разработки и внедрению (DevSecOps)			и	и	и								к				и	и		и										и					
Специалист по анализу защищенности									О и	О и	О и					О и		и		и К	и								и	и	и				
Специалист по автоматизации сбора и обработки событий ИБ				и	и	и		О и				и	и					и		и	и		и		и	и								
Специалист по мониторингу инцидентов в инфраструктуре								и	и	и	и							и		и	и		О и		О и	и								
Специалист по мониторингу инцидентов в анти-фрод системе								и	и	и								и		и	и		О и	О и		и								
Специалист по расследованию инцидентов								и										и	и	и	и			и		и	и							
Администратор ключевой защиты		и		и	и	и	и	и					и	и			и	и																
Администратор УЦ		и		и	и	и	и	и					и		и		и	и																
Специалист по защите информации		и				и	и			и		и	и	и	и	и		и	и	и	и		и		и	и	и	и					и	

О – организация
И – исполнение
К – контроль

Матрица полномочий на примере жизненного цикла информационной системы

	Проектирование систем ИБ	Проектирование подсистем ИБ и выработка требования ИБ для информационных систем	Внедрение систем ИБ и подсистем ИБ в информационных системах	Анализ защищенности информационных систем	Разработка эксплуатационной документации на средства обеспечения ИБ	Анализ угроз информационной безопасности	Организация и контроль процесса управления рисками ИБ	Выявление, идентификация и оценка рисков	Сбор и регистрация информации о выявленных рисках	Мониторинг рисков информационной безопасности и контроль показателей уровня рисков ИБ	Проведение проверок по выполнениям требований ИБ	Анализ ПО и модулей ПО на НДВ	Анализ заявок на сетевой доступ	Анализ заявок на доступ ТУЗ и сервисов
Методолог						О И К	О И К	И			И			
Эксперт по рискам ИБ						О И К	О И К	О И К	О И	О И К				
Администратор доступов	И	И	И			И		И	И				И	И
Архитектор средств защиты сетевой инфраструктуры	О И	О И	О И			И	И						И	И
Архитектор средств защиты информационных систем	О И	О И	О И			И	И						И	И
Аудитор технологических процессов (технолог)	И	И	О И		И	И	И	И	И				И	И
Специалист по процессам безопасной разработке и внедрению (DevSecOps)	И	И			И	И		И						
Специалист по анализу защищенности				О И		И		И К	И		И	И		
Специалист по автоматизации сбора и обработки событий ИБ	И	И	И			И		И	И					

О – организация
И – исполнение
К – контроль

03

Региональный функции

Набор сотрудников головных подразделений в регионах

- Дефицит квалифицированного персонала в Москве

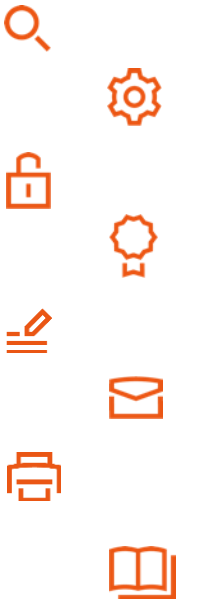
- Высокий уровень ожидания по уровню ЗП

- Запущен проект по регионализации, в рамках которого разработаны подходы по размещению в региональном отделении при оформлении в ГО

- Возможность набора сотрудников, которые не готовы релоцироваться, снижение затрат на релокацию

- Возможность размещения в ресурсном центре ИТ, что несет взаимные выгоды для ИТ и ИБ

Действия региональных подразделений ОЗИ ИБ в рамках централизованных процедур



- Участие в централизованных процессах мониторинга и реагирования на инциденты ИБ (события ИБ с признаками инцидента ИБ)
- Выявление инцидентов ИБ в зоне ответственности своего подразделения
- Участие в процессах внутреннего сканирования инфраструктуры соответствующих филиалов/региональных подразделений
- Участие в процессах управления доступом к информационным ресурсам/системам/ролям (в том числе на стадиях согласования, исполнения, ревизий прав доступа)
- Участие в проверках ИБ и мероприятиях по повышению осведомленности (Security Awareness)
- Выполнение задач по обеспечению криптографической защите информации в регионе
- Обеспечения выполнения требований лицензированной деятельности (ФСТЭК/ФСБ)
- Участие в прочих процессах обеспечения ИБ как подразделения ИБ на «местах»

Текущие задачи региональных отделов защиты информации

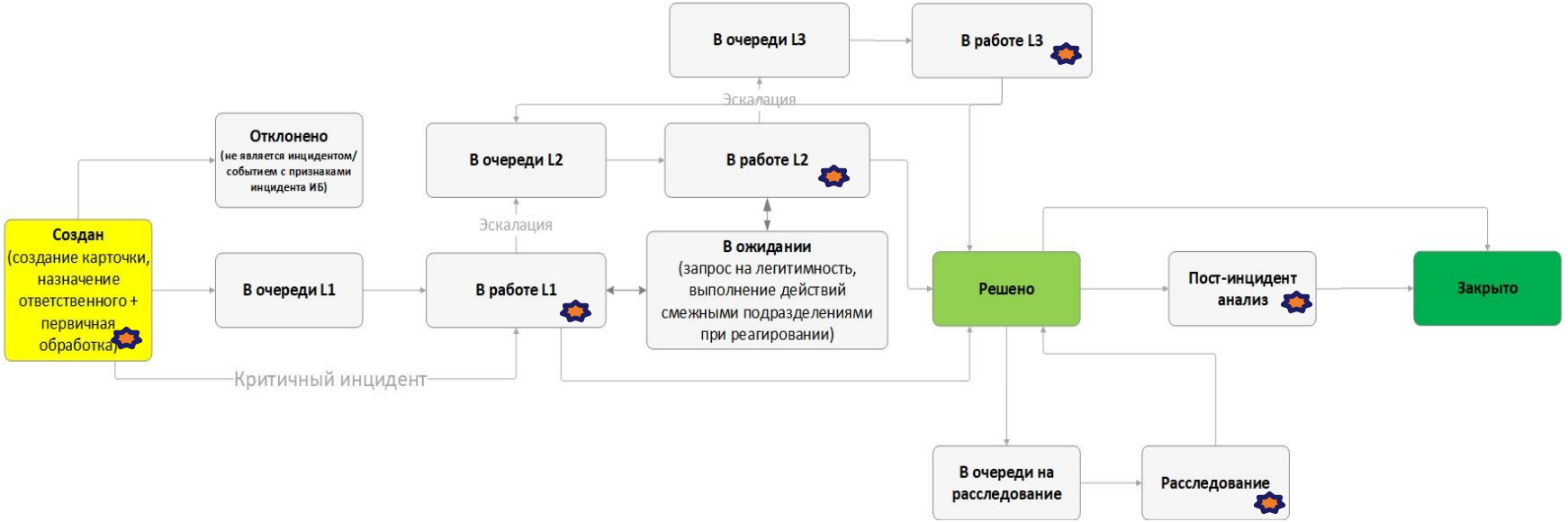
Функциональные обязанности сотрудников ОЗИ в соответствии с матрицей полномочий

- Методологическая помощь структурным подразделениям
- Внедрение систем ИБ и подсистем ИБ в информационных системах
- Администрирование и сопровождение систем ИБ
- Аудит защищенности сетевой инфраструктуры
- Контроль исполнения стандартов настроек
- Установка и настройка средств защиты в информационных системах
- Организация учета и распространения средств криптографической защиты
- Анализ защищенности информационных систем
- Анализ угроз информационной безопасности
- Организация и контроль процесса управления рисками ИБ
- Выявление, идентификация и оценка рисков
- Сбор и регистрация информации о выявленных рисках
- Мониторинг, выявление и регистрация инцидентов ИБ
- Реагирование на инциденты ИБ
- Расследование инцидентов ИБ
- Подготовка отчетов по инцидентам ИБ
- Проведение проверок по выполнениям требований ИБ
- Анализ заявок на сетевой доступ

Функциональные обязанности сотрудников ОЗИ для управления и отчетности

- Контроль работоспособности антивирусных средств
- Согласование заявок на предоставление (отзыв) доступа к информационным ресурсам
- Контроль записи информации на СМНИ
- Сопровождение и контроль систем обмена информации (Центральный Банк России, ФНС, ФТС, и т.д.)
- Проверка рабочих мест на предмет соблюдения ПОИБ (Включено хранение документов, ключей, печатей штампов, настройка ПК: BIOS, запрет загрузки, пломбы, контроль установленного ПО) Филиала
- Ознакомление сотрудников с ВНД
- Выдача ключевых носителей
- Выпуск ключей для защищенного обмена информацией
- Подготовка документации для выполнения требований ФСТЭК/ФСБ для помещений, СКС, сетевого оборудования, АРМ и СЗИ
- Контроль функционирования системы DLP на рабочих станциях
- Контроль использования сетевых ресурсов
- Контроль использования Интернет-ресурсов
- Контроль процедуры резервного копирования на серверах филиала
- Проведение консультаций (в т.ч. телефонных) по порядку обращения с паролями доступа к компьютерным системам и дистанционной работе, по противодействию вредоносному ПО на рабочих станциях пользователей филиала
- Обучение и тестирование сотрудников
- Контроль функционирования СКЗИ
- Выпуск НКЭП/УКЭП
- Имплементация требований для помещений, СКС, сетевого оборудования, АРМ и СЗИ

Основные этапы и статусная модель обработки инцидентов, участие региональных подразделений

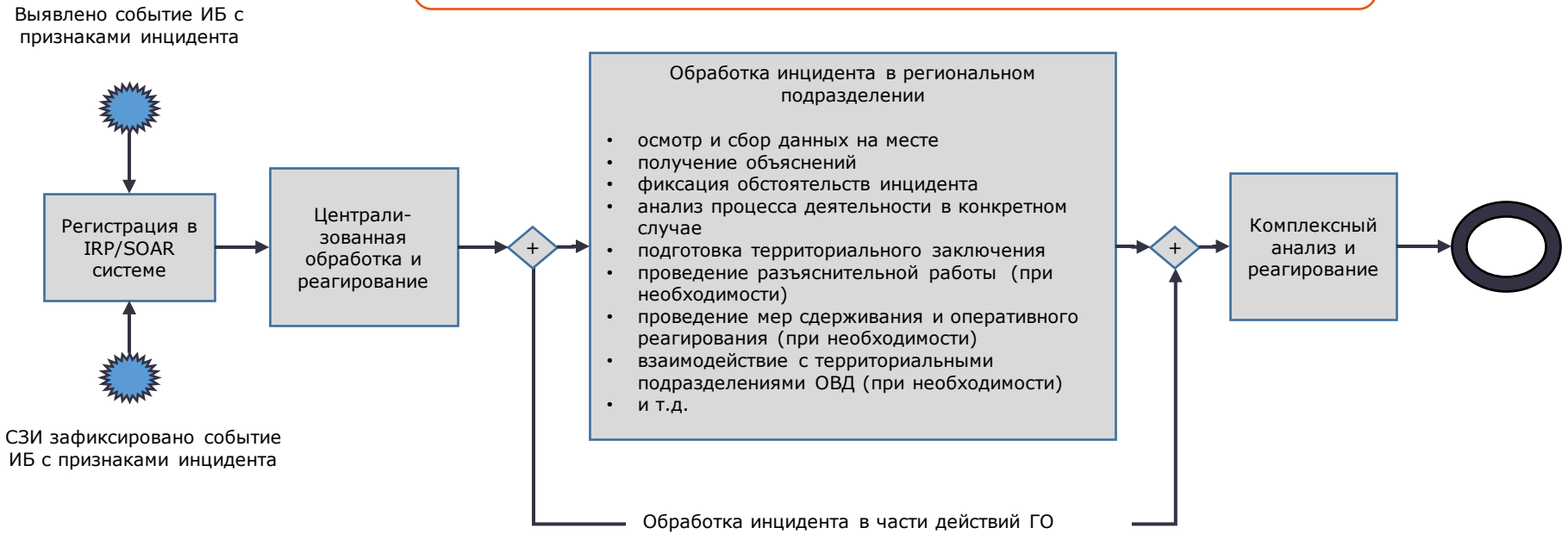


Участие региональных подразделений в обработке инцидентов (событий ИБ с признаками инцидента)

Сценарий распределенной обработки инцидентов с задействованием региональных подразделений

«На земле виднее»

Условия привлечения регионального подразделения – необходимость проверки рабочего места работника в региональном подразделении, проведение непосредственного взаимодействия с работниками (задействованными в инциденте) и их руководителями, необходимость получения данных с территориальных объектов, возникновение подозрения на инцидент в зоне ответственности филиала/регионального подразделения



Развитие функционала ОЗИ в части задач ГО

- Стараемся брать лучших в регионах
- Работа зачастую рутинная и однообразная
- Есть желание развиваться
- Есть желание активно участвовать в процессах обеспечения и развития ИБ по банку в целом
- Очные мероприятия для всех региональных ОЗИ и ИБ ГО раз в год
- Подключение общебанковским задачам в части ИБ

04

Дальнейшая регионализация

Условия для дальнейшей регионализации

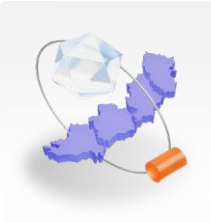
- Наличие специалистов в по необходимому направлению в регионе, в том числе наличие ВУЗов, готовящих профильных специалистов
- Возможно при наличии точек банка в требуемой локации
- Наличие возможности общеадминистративных и организационных функций в регионе
- Наличие лидера, который готов создавать и развивать регионализируемое направление
- Возможно выполнение полного перечня задач, относящихся к деятельности
- Регионализируются связанные функции

	Частичная регионализация функции	**Полная регионализация функции**
Методология	Не целесообразно	Не целесообразно
Мониторинг инцидентов в инфраструктуре	Часть функций уже в ОЗИ	Возможно при вынесении SOC
Анти-фрод мониторинг	Не целесообразно	Возможно при вынесении SOC и Call-центра в регион
Безопасность инфраструктуры	Частично реализуется в настоящее время	Не целесообразно
Технологическая экспертиза	Частично реализуется в настоящее время	Не целесообразно
Криптография	Часть функций уже в ОЗИ	Не целесообразно

05

Выводы

Выводы



Локальные задачи, включая обработку инцидентов, может осуществлять только специалист на месте

Организации должна быть готова к регионализации

Необходим обмен опытом и наращивание компетенций у региональных сотрудников

Можно брать сотрудников в регионы на задачи ГО при определенных условиях

Полный перевод функции в регион возможен в первую очередь при наличии компетентного персонала в регионе

ПСБ

psbank.ru

Спасибо!

Шведов
Сергей Владимирович

+7 (495) 546-44-44
+7 (916) 721-64-90
shvedovsv@psbank.ru