Современные подходы к обеспечению ИБ в банковской сфере

Дмитрий Породин
Ведущий инженер

ЭЛВИС-ПЛЮС

Основные проблемы ИБ в банковской сфере

- Развитие и совершенствование технологий и методов современных атак
- Сложность и комплексность требований законодательства, нормативных документов регуляторов, требований международных платежных систем
- Утечки банковской тайны и ПДн, защита от «инсайдеров»
- Сложность автоматизированной банковской системы, проблемы управления доступом к данным
- Взаимодействие с сетью общего пользования Интернет
- Необходимость создания нормативной базы по ИБ

Тенденции развития информационных угроз

- Изменение операционной среды — развитие социальных сетей, видеохостингов, облачных сервисов.
- Формирование хорошо организованной квалифицированной среды хакеров — «экосистема киберпреступности».
- Использование взломанных сайтов для распространения вредоносного кода.
- Перенос акцентов атаки на приложения и пользователей.
- Атаки на сети соперников на рынке — как часть конкурентной борьбы.

Существующие угрозы

- Прямые финансовые потери — взлом внешними злоумышленниками систем дистанционного банковского обслуживания, кража денежных средств у клиентов Банка.
- Репутационные риски — нарушение функционирования или взлом публичных банковских сервисов (веб-сайт Банка, система электронной почты).
- Утечка конфиденциальной информации (банковская тайна, персональные данные) — использование уязвимостей веб-браузеров и заражение вредоносным кодом рабочих станций сотрудников Банка.

Нормативные документы по ИБ в банковской сфере

- Федеральный закон «О национальной платежной системе» 161-ФЗ, Положение Банка России №382-П, Указание Банка России №3361-У
- Федеральный закон «О персональных данных» 152-ФЗ, Постановление Правительства РФ №1119, приказ ФСТЭК №21, приказ ФСБ №378
- Комплекс стандартов Банка России СТО БР ИБСС
- Положение Банка России о внутреннем контроле №242-П
- Положение Банка России №379-П «О бесперебойности функционирования платежных систем и анализе рисков в платежных системах»
- Письмо Банка России №47-Т «О Методических рекомендациях по проведению проверки и оценки организации внутреннего контроля в кредитных организациях»
- Письмо Банка России №49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»
- PCI DSS

Финансовые потери при утечках информации

- В 2011 году компании потратили на ликвидацию последствий утечек более 500 млн. долл. Публично обнародована информация о потерях компаний в размере 14,8 млн. долл.
- Прямые убытки кредитно-финансовых организаций от утечек в первом полугодии 2012 года составили чуть более 2 млрд долл. Скомпрометировано более 2 млн записей, в том числе финансовые и персональные данные.
- В 2013 году в мире зафиксировано, обнародовано в СМИ и зарегистрировано случаев утечек на 22% больше, чем за прошлый год

Сложность внутренней нормативной базы по ИБ

- Политика ИБ
- Частные политики в области ИБ:
  - Управление доступом к ИС
  - Взаимодействие с сетью общего пользования Интернет
  - Управление инцидентами ИБ
  - Защита от вредоносного кода
  - Использование съемных носителей
  - и т.д.
- План ОНиВД
- Регламенты (порядки)
- Инструкции

Общая структура процессов управления СОИБ

Группа процессов поддержки принятия решений

- Организация работ по реализации и выполнению планов внедрения развития
- Приятие решений по вопросам эксплуатации
- Организация работ по совершенствованию СОИБ
- Организация работ по обучению и повышению квалификации

Группа процессов мониторинга и контроля состояния ИБ

- Мониторинг и анализ событий ИБ
- Контроль действий пользователей
- Контроль защищенности ИР
- Обнаружение и предотвращение вторжений

Группа процессов анализа состояния ИБ

- Идентификация, классификация и учет активов и ресурсов
- Обнаружение, реагирование и расследование инцидентов
- Проведение проверок состояния ИБ

Группа процессов контроля организации эксплуатации

- Контроль управления доступом к ИР
- Контроль управления конфигурациями
- Контроль управления обновлениями

Общая структура процессов реализации защитных мер СОИБ

Группа процессов реализации защитных мер инфраструктурного уровня

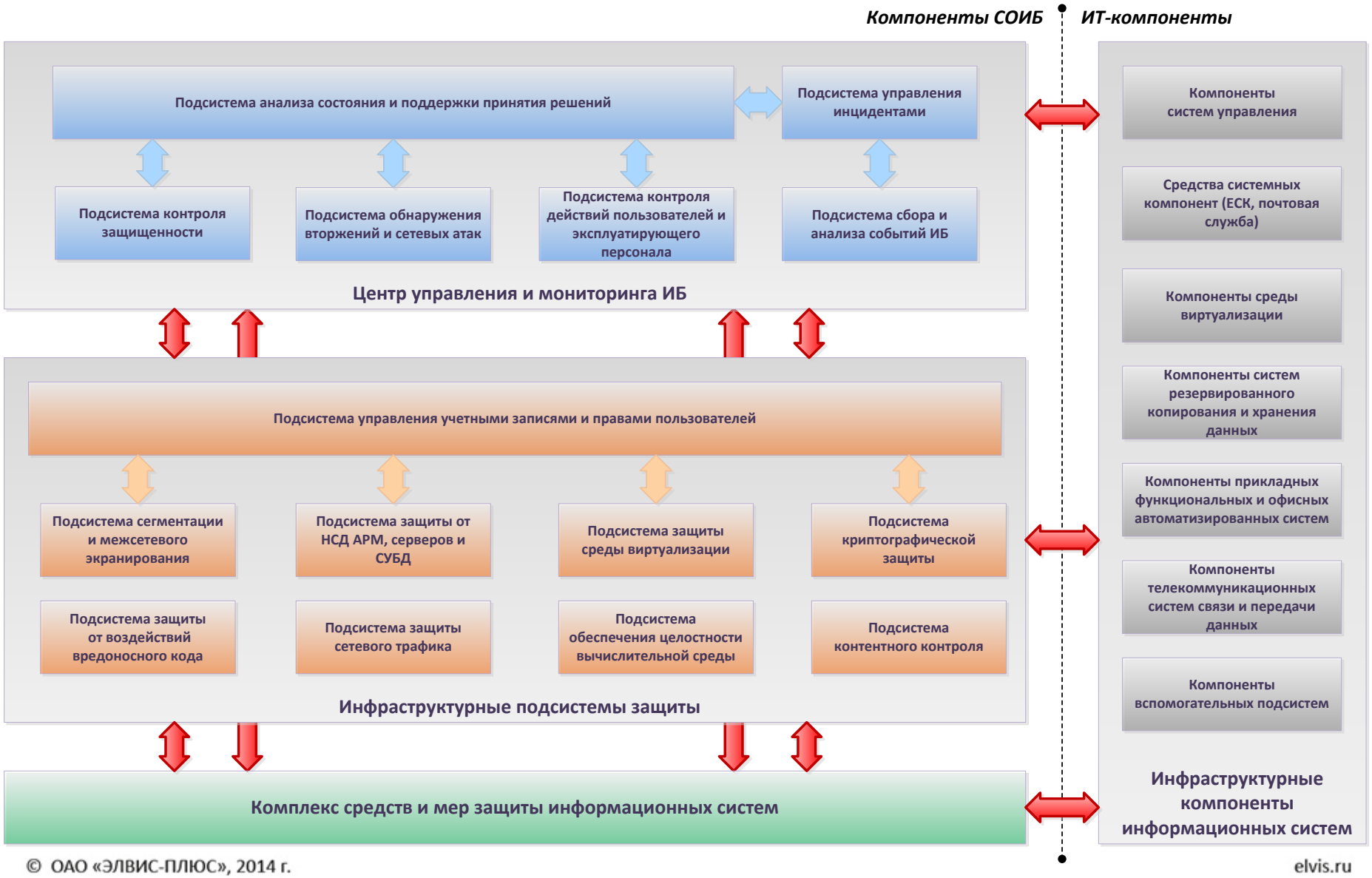
- Сегментация и межсетевое экранирование
- Защита сетевого трафика
- Защита от НСД АРМ, СУБД и серверов
- Защита от воздействий вредоносного кода
- Обеспечение целостности вычислительной среды
- Защиты среды виртуализации
- Контентный контроль
- Криптографическая защита

Группа процессов управления учетными записями и правами пользователей и персонала

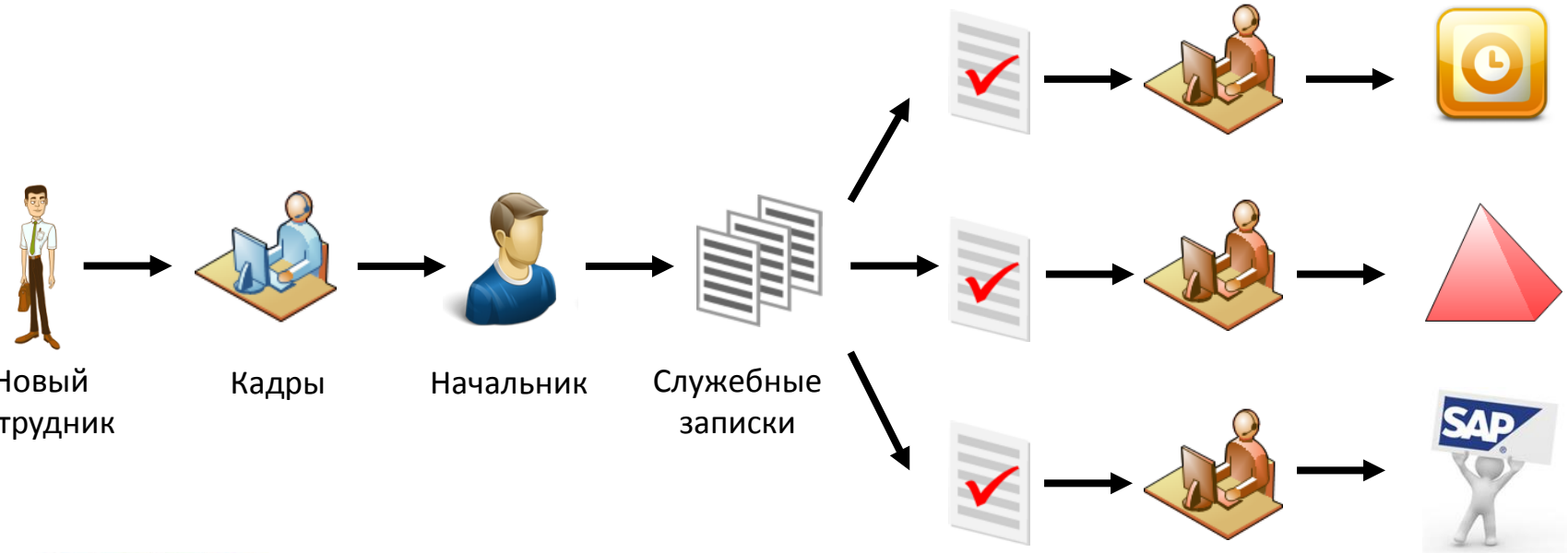
- Управление учетными записями и правами пользователей
- Управление доступом к оборудованию инфраструктуры

Группа процессов применения защитных мер информационных систем

Общая архитектура СОИБ

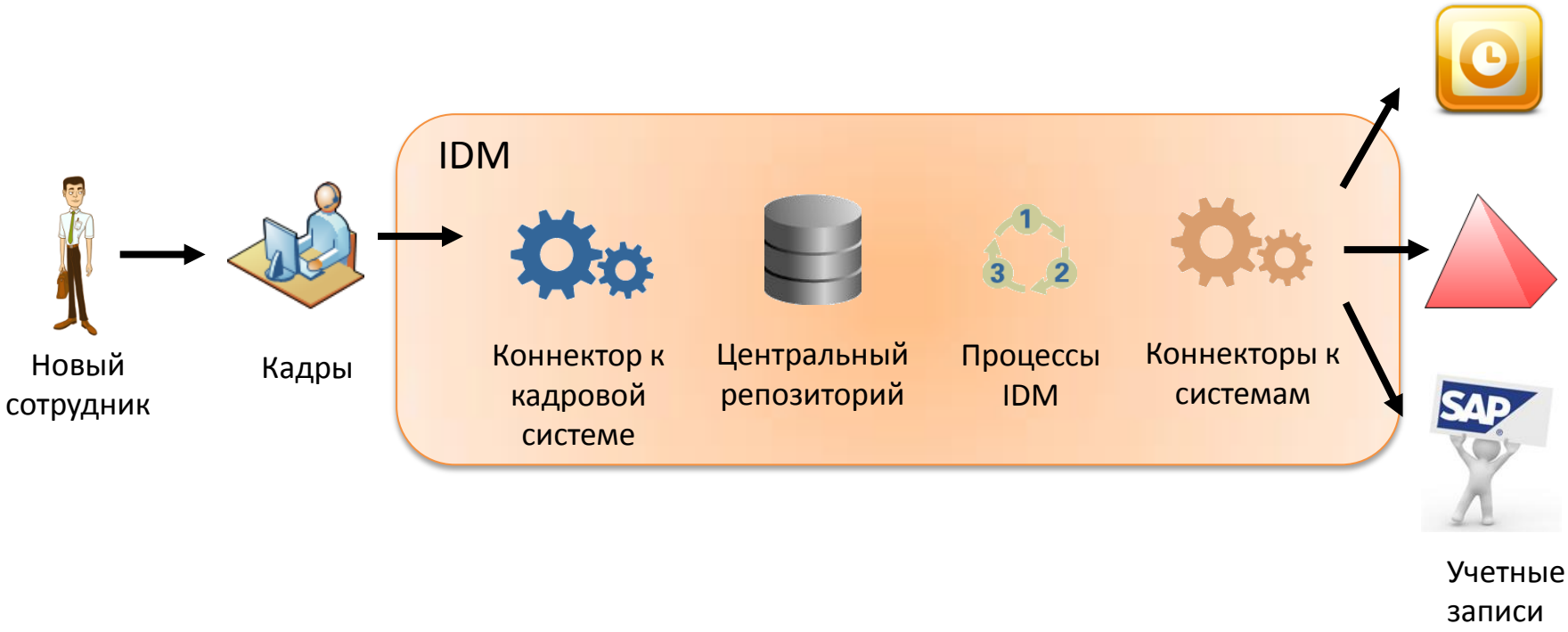


Подсистема управления учетными записями и правами пользователей



С момента приема на работу нового сотрудника и до момента выделения ему всех необходимых информационных ресурсов может пройти от нескольких дней до нескольких месяцев!

Подсистема управления учетными записями и правами пользователей

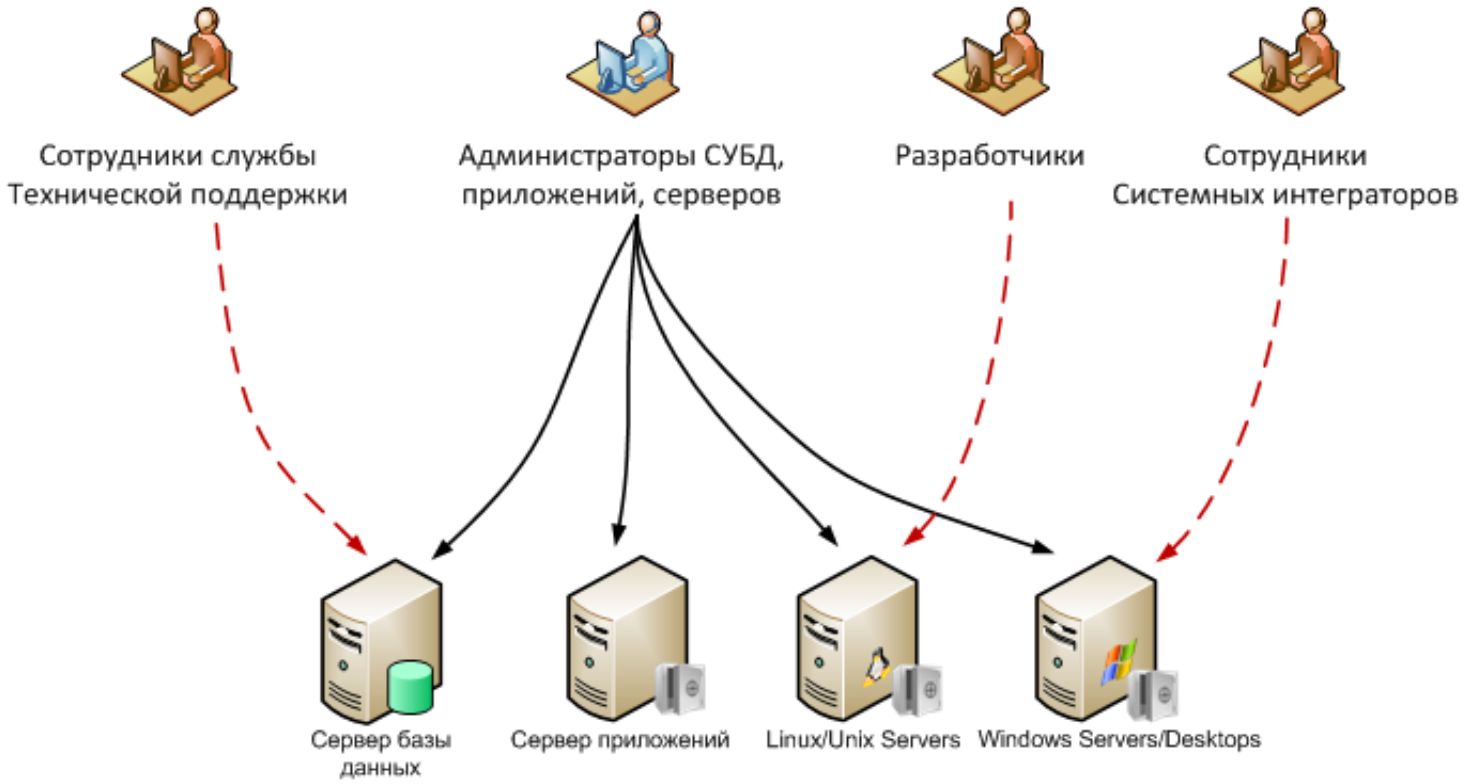


Новый сотрудник обеспечивается всеми необходимыми информационными ресурсами в день приема на работу.

Подсистема контроля действий пользователей и эксплуатирующего персонала

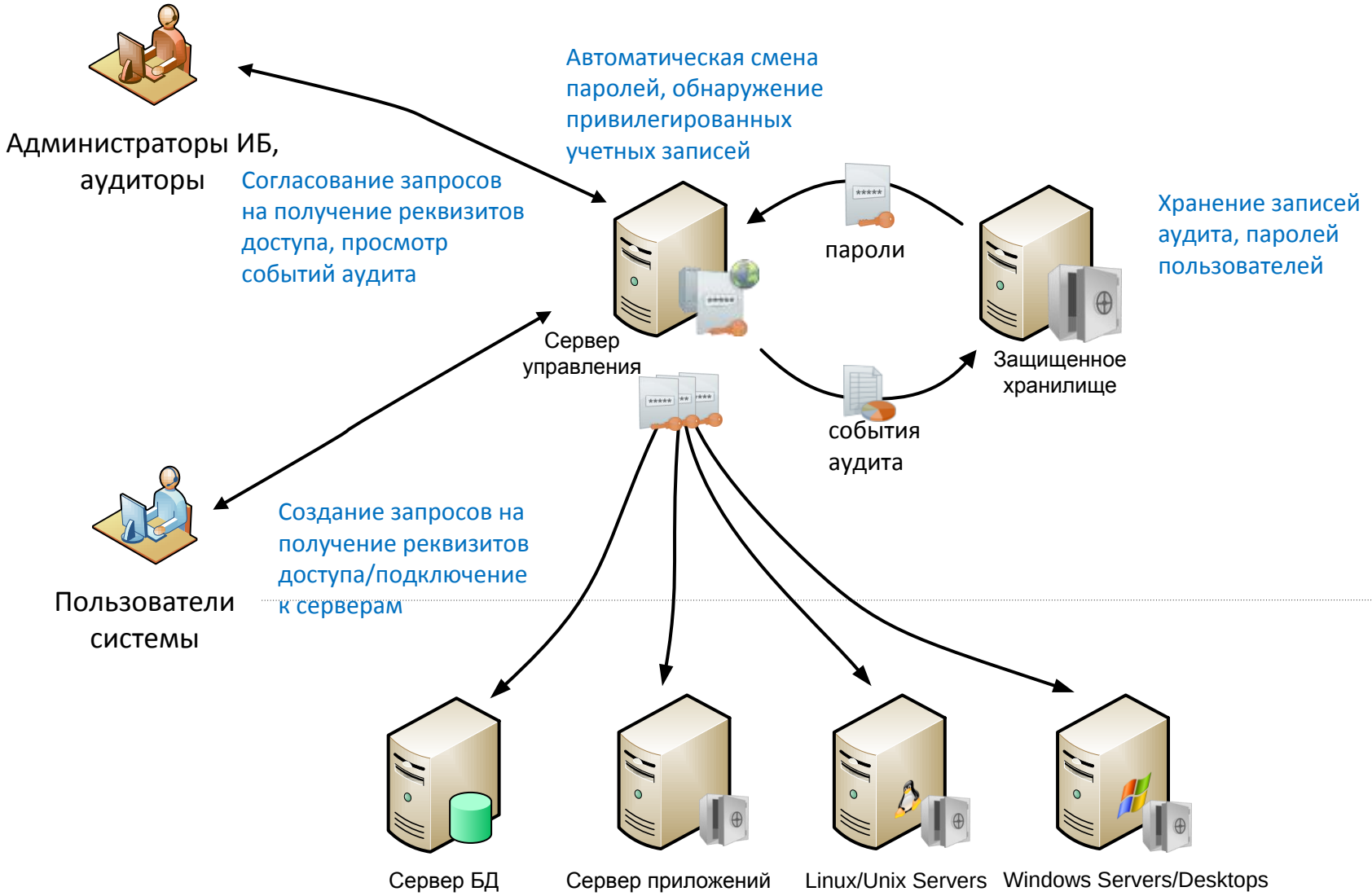
Результаты исследования Cyber-Privileged Account Security & Compliance Survey, Май 2013 (проводилось среди компаний корпоративного сектора, с количеством сотрудников более 5000)

Подсистема контроля действий пользователей и эксплуатирующего персонала

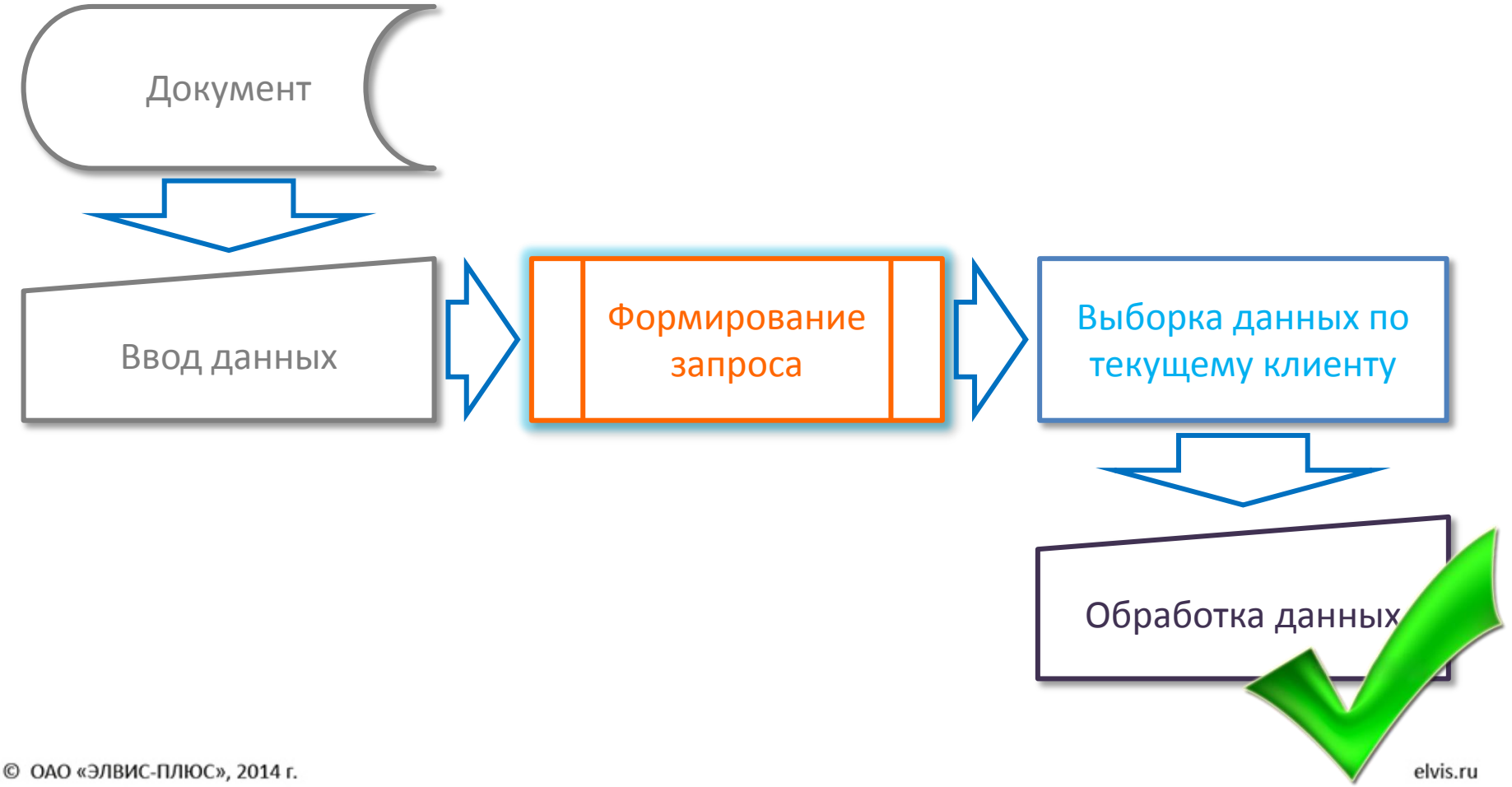


- Большое количество пользователей знает привилегированные учетные данные критичных ресурсов
- Отсутствие механизмов управления сессиями привилегированных пользователей
- Простые пароли привилегированных пользователей, редко изменяются

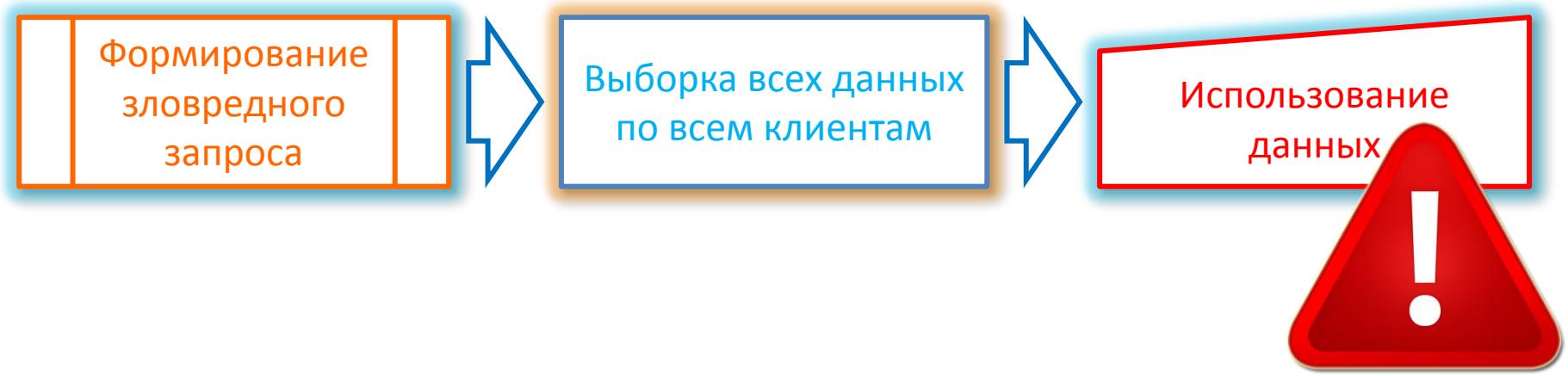
Подсистема контроля действий пользователей и эксплуатирующего персонала



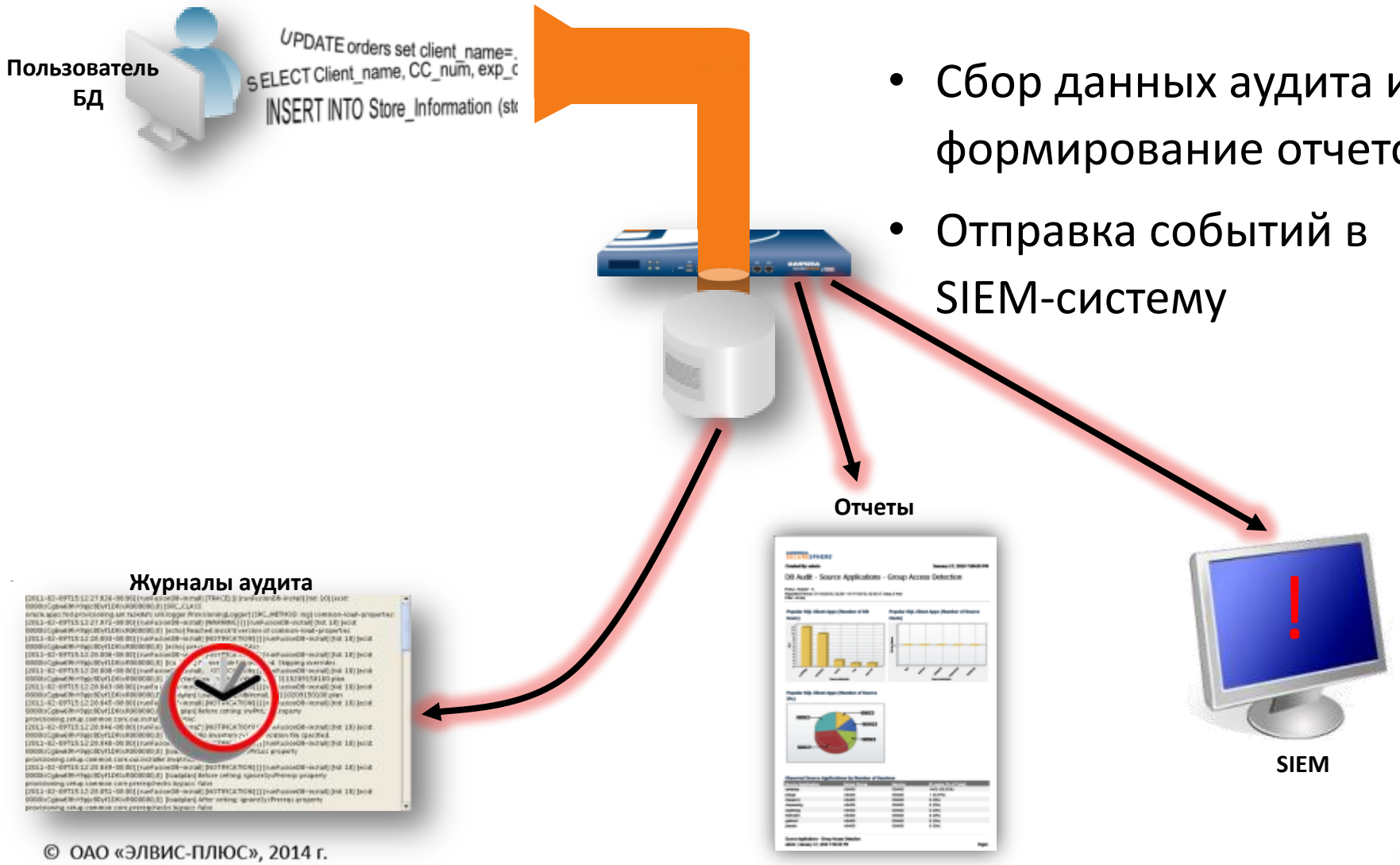
Подсистема защиты от НСД АРМ, систем управления базами данных и серверов



Подсистема защиты от НСД АРМ, систем управления базами данных и серверов



Подсистема защиты от НСД АРМ, систем управления базами данных и серверов



- Сбор данных аудита и формирование отчетов
- Отправка событий в SIEM-систему

Подсистема контентного контроля – управление печатью

- Сложно оценить расходы на печать без специализированных инструментов
- Средние расходы организации на печать составляют 3% от выручки (данные Gartner)
- Оптимизация расходов на печать позволяет уменьшить затраты организации на печать до 30% (данные Gartner)
- Печатные документы – основной канал утечки персональных данных в 2013 году в России (Аналитический Центр компании InfoWatch)

Подсистема контентного контроля – управление печатью

Подсистема анализа состояния ИБ и поддержки принятия решений

- Безопасность ИС банка должна обеспечиваться в рамках комплексной СОИБ, включающей в свой состав набор технических средств защиты и организационных мер, объединенных на основе выбранной модели управления
- В рамках комплексной СОИБ, адекватно компенсирующей актуальные риски ИБ, должны быть внедрены более 30 процессов ИБ (организационных мер), эффективная реализация которых невозможна без использования средств автоматизации

Подсистема анализа состояния ИБ и поддержки принятия решений

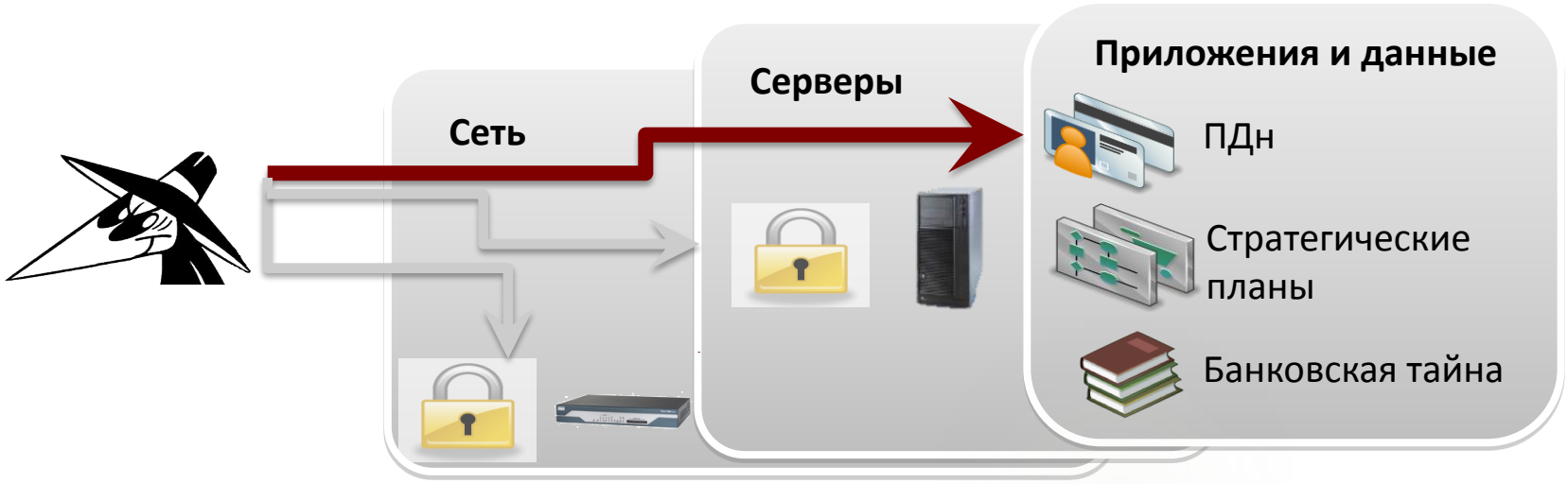
- Активы — автоматизация процессов учета, классификации и назначения владельцев защищаемых ИТ-активов
- Риски — автоматизация процессов менеджмента угрозами, уязвимостями и рисками ИБ
- Задачи — автоматизация процессов постановки и контроля за исполнением задач, связанных с обеспечением ИБ
- Ресурсы — автоматизация процессов менеджмента ресурсов системы ИБ, контроля их доступности и целесообразности их использования при решении задач по ИБ

Подсистема анализа состояния ИБ и поддержки принятия решений

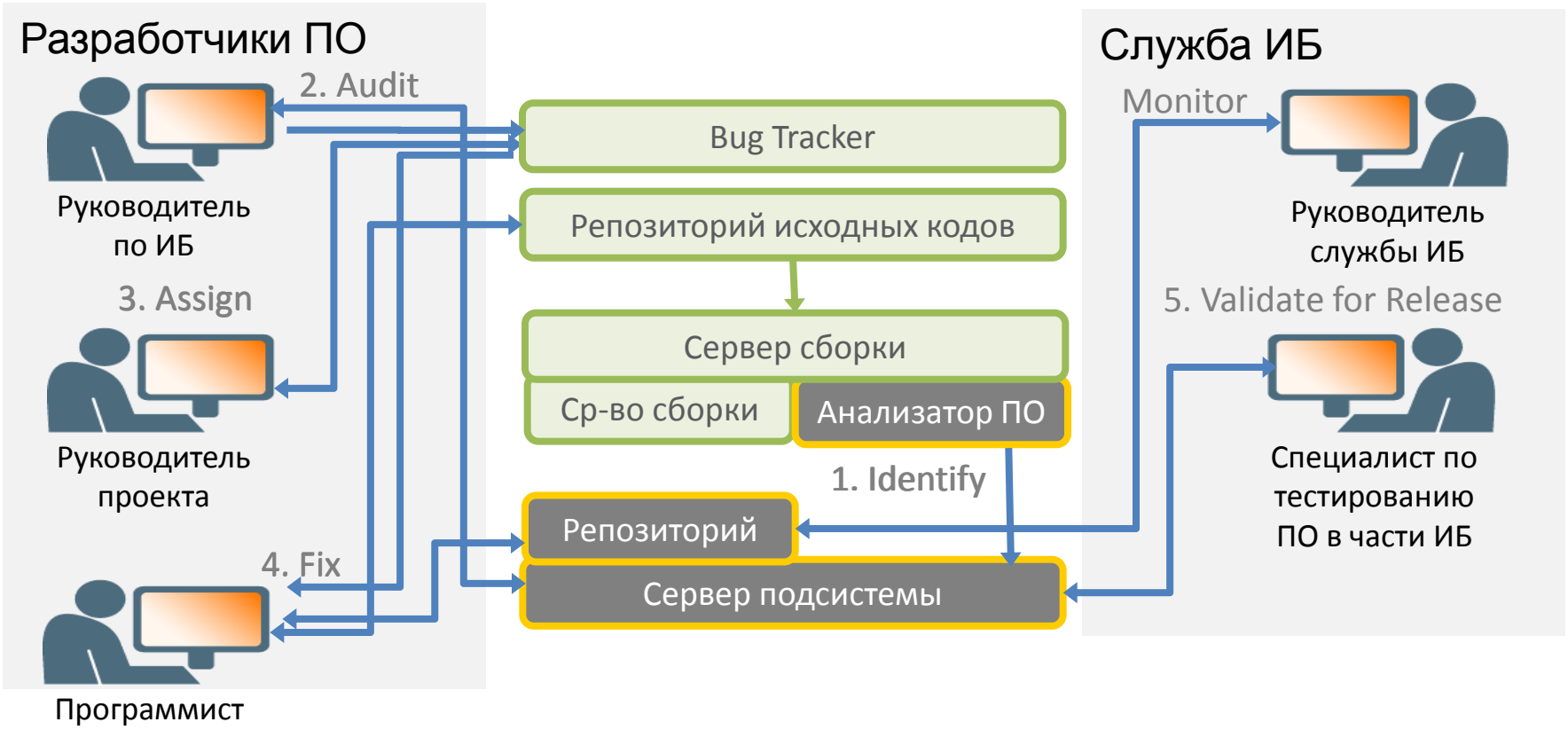
- Документы — автоматизация процессов создания, сбора, хранения, утверждения внешних и внутренних документов по ИБ, а также обеспечения справочной поддержки ИБ
- Аудит — автоматизация проведения и составления отчетности по результатам аудита СОИБ и анализа текущего состояния СОИБ
- Персонал — автоматизация проведения и составления отчетности по результатам аудита СОИБ и анализа текущего состояния СОИБ
- Жизненный цикл АБС — автоматизация процессов приобретения и разработки ИС и ИТ-сервисов, а также обеспечения ИБ при их создании и эксплуатации

Подсистема контроля защищенности – контроль исходного кода

- 75% нарушений связаны с недостатками в безопасности ПО (Gartner)
- 92% уязвимостей обнаруживаются в ПО (NIST)
- 86% успешных нарушений осуществляется на прикладном уровне (RSA)
- 99% веб-приложений имеют уязвимости (Cenzic)



Подсистема контроля защищенности – контроль исходного кода



Ваши вопросы?

Дмитрий Породин