БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Основные угрозы ИБ для коммерческих организаций

Скородумов Анатолий Валентинович

Заместитель директора –

Начальник управления по обеспечению информационной безопасности

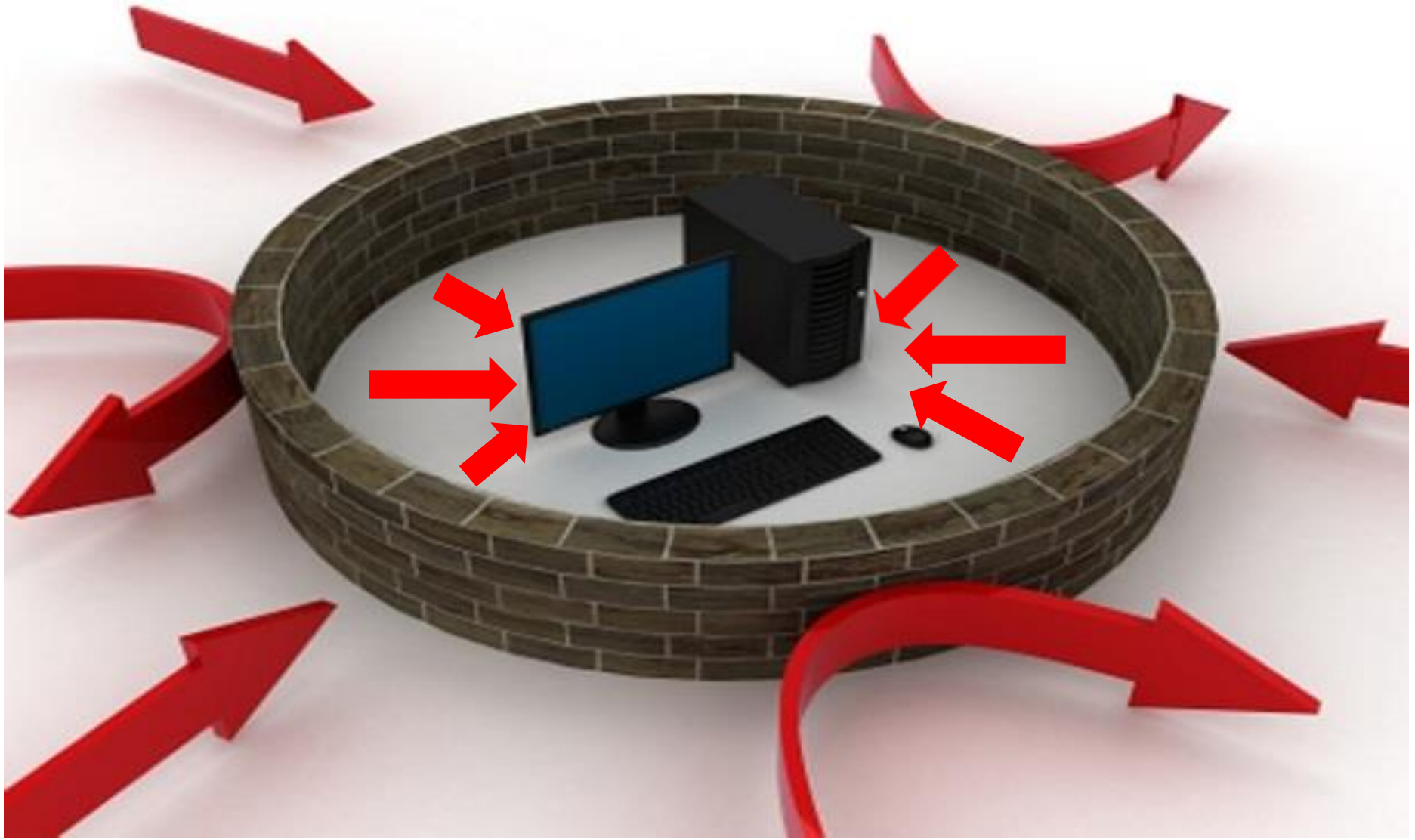
Основные факторы, стимулирующие развитие ИБ

- Рост количества инцидентов по ИБ и потерь от них
- Развитие законодательства в области ИБ
- Развитие ИТ в государственных организациях
- Наличие международных, российских и отраслевых стандартов по ИБ
- Изменения в структуре бизнеса
- Международные санкции в отношении России

Основные ИТ-тренды, влияющие на ИБ

- Мобильность
- Облака
- Большие данные
- Социальные сети
- Виртуализация
- Аренда ЦОД
- Аутсорсинг ИТ
- Работа сервисов в режиме 24*7
- Повышение общего уровня компьютерной грамотности работников

Внешние и внутренние угрозы



Актуальные внешние угрозы

- Атаки на системы дистанционного обслуживания
- Утечки через уязвимости в публичных веб-приложениях
- DDOS-атаки
- Таргетированные (целевые) атаки
- Информационные атаки
- Угрозы, связанные использование мобильных устройств
- Угрозы, связанные с использованием облачных сервисов

Защита от внешних угроз

- Использование систем фрод-анализа для систем дистанционного обслуживания
- Регулярный анализ систем дистанционного обслуживания на уязвимости
- Проведений внешних и внутренних тестов на проникновение
- Использование принципов безопасного программирования
- Мониторинг интернета для оперативного выявления информационных атак
- Использование МДМ-систем для управления мобильными устройствами

Актуальные внутренние угрозы

- Утечка критичных данных
- Злоупотребления со стороны работников организации (хищения, приписки)
- Ошибки и умышленные действия администраторов

Защита от внутренних угроз

- Использование системы защиты от утечки (DLP)
- Мониторинг запросов пользователей к БД
- Мониторинг обращений пользователей к общим каталогам
- Использование систем фрод-анализа для выявления внутренних мошенников
- Использование систем управления правами доступа
- Повышение осведомленности сотрудников в вопросах ИБ
- Использование систем контроля за работой привилегированных пользователей

Средства выявления аномалий как основа СОИБ

- Аномалии в запросах пользователя в АС
- Аномалии сетевой активности
- Аномалии в работе с приложениями
- Аномалии при работе с файлами, с устройствами внешнего хранения данных
- Аномалии в выполнении бизнес задач

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Скородумов Анатолий Валентинович

E-Mail: Skorodumov@mail.ru

Телефон (812) 329-50-64

Благодарю за внимание!