РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЛЕКЦИЯ 3. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фрагментарный подход
направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т. п.

Комплексный подход
ориентирован на создание защищенной среды обработки информации в КС, объединяющей в единый комплекс разнородные меры противодействия угрозам.
Недостаткам этого подхода относятся: ограничения на свободу действий пользователей КС, чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законодательные
стандарты, законы, нормативные акты и т. п.

Программно-технические
конкретные технические меры
- идентификация и проверка подлинности пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование;
- обеспечение высокой доступности.

Административно-организационные действия общего характера, предпринимаемые руководством организации, и конкретные меры безопасности, касающиеся людей.
Группы организационных мер:
- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетание законодательных, административно-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам являются тем фундаментом, на котором строится вся система защиты информационных систем.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАДАЧИ КОМПЛЕКСНОЙ ЗАЩИТЫ

- проанализировать угрозы информационной безопасности для КИС;
- разработать политику информационной безопасности;
- защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации;
- гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Интернета, а также общения с пользователями этих сетей;
- защитить отдельные наиболее коммерчески значимые информационные системы независимо от используемых ими каналов передачи данных;
- предоставить защищенный удаленный доступ персонала к информационным ресурсам корпоративной сети;
- обеспечить надежное централизованное управление средствами сетевой защиты.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ В БС

Общие принципы

-Своевременность обнаружения проблем;

- Прогнозируемость развития проблем;

-Оценка влияния проблем на бизнес-цели;

- Адекватность защитных мер;

- Эффективность защитных мер;

-Использование опыта при принятии и реализации решений;

-Непрерывность принципов безопасного функционирования;

-Контролируемость защитных мер

Специальные принципы

- Определенность целей;

- Знание своих клиентов и служащих ;

-Персонификация и адекватное разделение ролей и ответственности;

-Адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки;

- Доступность услуг и сервисов;

-Наблюдаемость и оцениваемость обеспечения информационной безопасности;

Специальный принцип «знание своих клиентов и служащих» (Financial services - Information security guidelines)

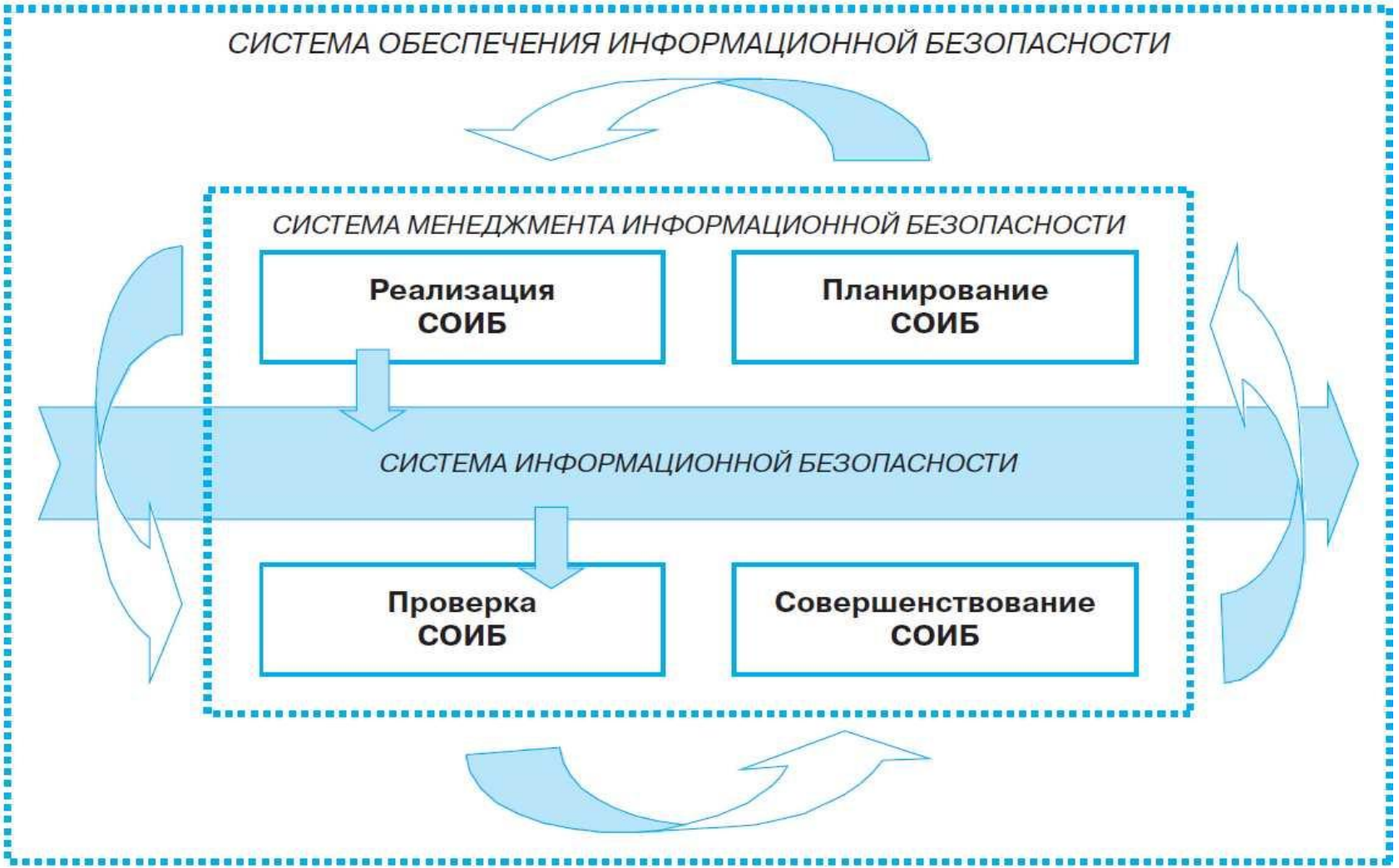
«Знать своего клиента» (Know your Customer): принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов [ISO TR 13569]

«Необходимо знать» (Need to Know): принцип безопасности, который ограничивает доступ к информации и ресурсам по обработке информации тем, кому требуется выполнять определенные обязанности [ISO TR 13569].

«Знать своего служащего» (Know your Employee): принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью [ISO TR 13569]

«Двойное управление» (Dual Control): принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий того, чтобы два лица независимо предпринимали некое действие до завершения определенных транзакций [ISO TR 13569].

СОИБ ОРГАНИЗАЦИИ БС РФ



ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

цели обеспечения ИБ

- повышение стабильности функционирования Банка в целом;
- достижение адекватности мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности;
- повышение доверия к Банку со стороны клиентов, контрагентов, партнеров, инвесторов и общественности в целом, повышение рейтинга Банка и его инвестиционной привлекательности;

Объектами защиты с точки зрения информационной безопасности в Банке являются:

- платежная информация;
- персональные данные клиентов Банка;
- банковский информационный технологический процесс;
- электронные базы данных Банка;
- различного рода носители защищаемой информации.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Политика информационной безопасности

Шангин В.
совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов

Стандарт Банка России
Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации БС РФ в целом

Можно построить такую политику безопасности, которая будет устанавливать, кто имеет доступ к конкретным активам и приложениям, какие роли и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности.

Стандарт Банка России
частная политика ИБ - Документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности БС РФ.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

РАЗДЕЛЫ ПОЛИТИКИ БЕЗОПАСНОСТИ

ОПИСАНИЕ ПРОБЛЕМЫ

продемонстрировать сотрудникам организации важность защиты сетевой среды

ПОЗИЦИЯ ОРГАНИЗАЦИИ

Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности.

САНКЦИИ

Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.

ОБЛАСТЬ ПРИМЕНЕНИЯ

В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. Политика ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков

РАСПРЕДЕЛЕНИЕ РОЛЕЙ И ОБЯЗАННОСТЕЙ

За реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи сети

ТРИ УРОВНЯ ПОЛИТИК БЕЗОПАСНОСТИ

ВЕРХНИЙ УРОВЕНЬ

решения, затрагивающие организацию в целом.

-формулировка целей;
-формирование или пересмотр КПОИБ;
-обеспечение материальной базы;
-формулировку управленческих решений

СРЕДНИЙ УРОВЕНЬ

решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией.

НИЖНИЙ УРОВЕНЬ

В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной. Чем детальнее правила, чем более четко и формально они изложены, тем проще поддержать их выполнение программно-техническими мерами. Обычно наиболее формально задаются права доступа к объектам.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СТРУКТУРА ПОЛИТИКИ БЕЗОПАСНОСТИ

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СПЕЦИАЛИЗИРОВАННЫЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

ПОЛИТИКИ, ЗАТРАГИВАЮЩИЕ ЗНАЧИТЕЛЬНОЕ ЧИСЛО ПОЛЬЗОВАТЕЛЕЙ

- политика допустимого использования;
- политика удаленного доступа к ресурсам сети;
- политика защиты информации;
- политика защиты паролей и др.

.

ПОЛИТИКИ, СВЯЗАННЫЕ С КОНКРЕТНЫМИ ТЕХНИЧЕСКИМИ ОБЛАСТЯМИ

- политика конфигурации межсетевых экранов;
- политика по шифрованию и управлению криптоключами;
- политика безопасности виртуальных защищенных сетей VPN;
- политика по оборудованию беспроводной сети и др.

ПОЛИТИКА ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ

ЦЕЛЬ

установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников с целью защиты корпоративных ресурсов и собственной информации.

ДОЛЖНА УСТАНОВИТЬ:

-ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;

-возможность читать и копировать файлы, которые не являются собственными документами пользователей, но доступны им;

- уровень допустимого использования для электронной почты и веб-доступа.

могут быть политики допустимого использования для компьютеров, передачи данных, коммуникаций электронной почты, портативных персональных компьютеров, веб-доступа и др.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛИТИКА УДАЛЕННОГО ДОСТУПА

ЦЕЛЬ

установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании

ДОЛЖНА ОПРЕДЕЛИТЬ:

-какие методы разрешаются для удаленного доступа;
-каковы ограничения на данные, к которым можно получить удаленный доступ;
-кто может иметь удаленный доступ.

-Защищенный удаленный доступ должен быть строго контролируемым.
-Применяемая процедура контроля должна гарантировать, что доступ к надлежащей информации или сервисам получат только прошедшие проверку люди.
-Сотрудник компании не должен передавать свои логин и пароль никогда и никому, включая членов своей семьи.
- Управление удаленным доступом не должно быть настолько сложным, чтобы это приводило к возникновению ошибок.

ПРОЦЕДУРЫ БЕЗОПАСНОСТИ

ЦЕЛЬ
определяют, как защитить ресурсы и каковы механизмы исполнения политики, то есть как реализовывать политики безопасности

ПРОЦЕДУРА УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ
определяет:
- кто имеет полномочия выполнять изменения конфигурации аппаратного и программного обеспечения;
-как тестируется и инсталлируется новое аппаратное и программное обеспечение;
как документируются изменения в аппаратном и программном обеспечении;
-кто должен быть проинформирован, когда вносятся изменения в аппаратном и программном обеспечении.

ПРОЦЕДУРА РЕАГИРОВАНИЯ НА СОБЫТИЯ
определяет:
-каковы обязанности членов команды реагирования;
-какую информацию следует регистрировать и прослеживать;
- как обрабатывать исследование отклонений от нормы и атаки вторжения;
- кого уведомлять и когда;
-кто может выпускать в свет информацию и какова процедура ее выпуска;
- как должен выполняться последующий анализ и кто будет в этом участвовать.

ШАГИ ПО РАЗРАБОТКЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

-создание команды по разработке политики;
-принятие решения об области действия и целях политики;
-принятие решения об особенностях разрабатываемой политики;
-определение лица или органа для работы в качестве официального интерпретатора политики.

анализ требований бизнеса (какие компьютерные и сетевые сервисы требуются для бизнеса и как эти требования могут быть удовлетворены при условии обеспечения безопасности?)

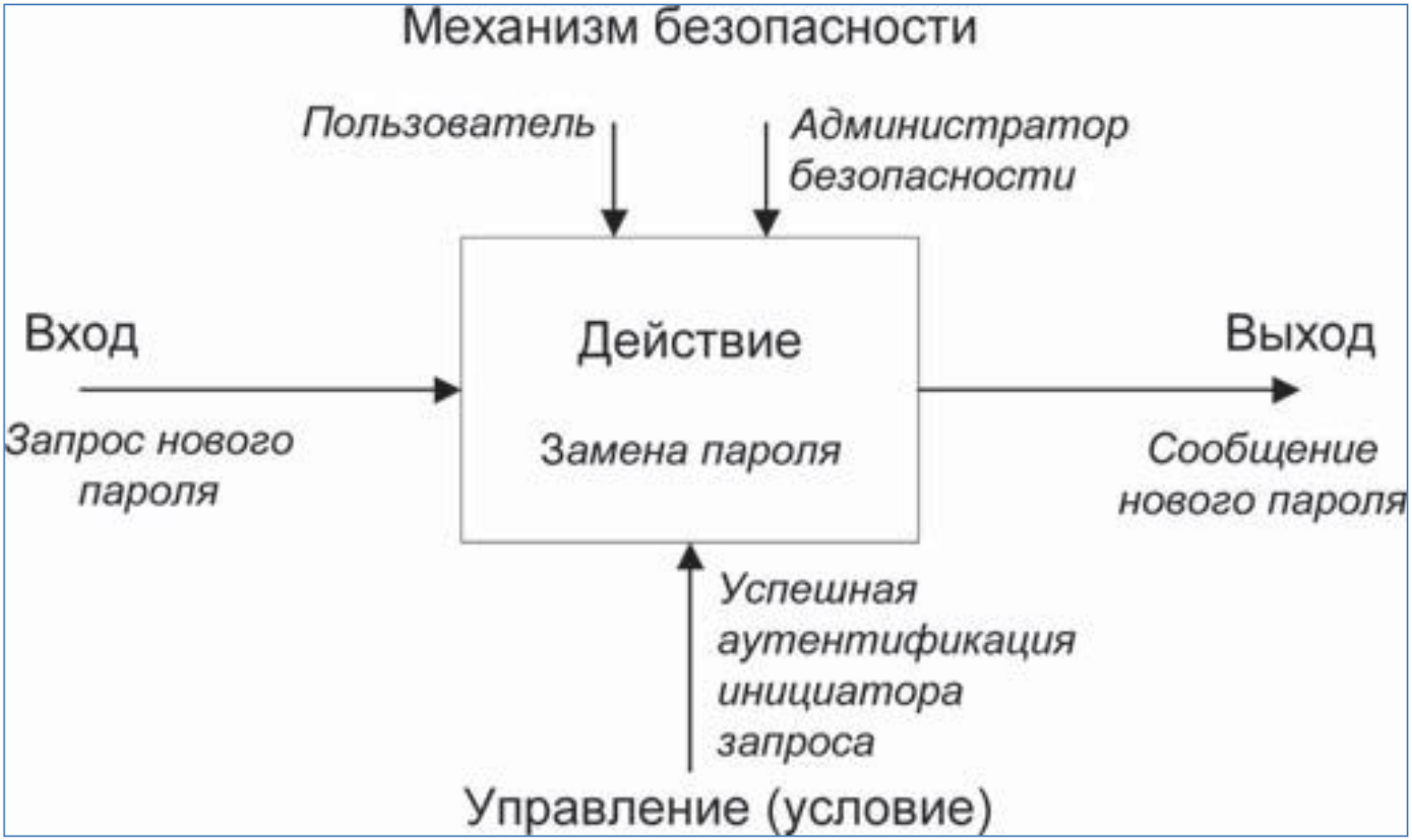
Установление уровня безопасности
стоимость защиты конкретного актива не должна превышать стоимости самого актива

анализ рисков;
-идентификация и оценка стоимости технологических и информационных активов;
-анализ тех угроз, для которых данный актив является целевым объектом;
- оценка вероятности того, что угроза будет реализована на практике;
- оценка рисков этих активов

Регулярная переоценка рисков

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОЦЕСС В ИБ



РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФИЗИЧЕСКАЯ И ЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЦЕЛЬ ФБ

заключается прежде всего в определении тех компонентов компьютерной среды, которые должны быть физически защищены

КОМПОНЕНТЫ ФБ:

- центральные процессоры и системные блоки;
- компоненты инфраструктуры локальной сети LAN, такие как системы управления LAN, мосты, маршрутизаторы, коммутационные коммутаторы, активные порты и др.;
-системы, связанные с LAN;
-медиапамять.

ТИПЫ ОБЛАСТЕЙ ФБ

-***открытые области,*** в которые могут допускаться все сотрудники компьютерной среды;

-***контролируемые области,*** которые могут и должны быть закрыты, когда находятся без присмотра;

- ***особо контролируемые области,*** куда ограничен доступ даже зарегистрированным авторизованным пользователям.

КОМПОНЕНТЫ ЛБ

средства безопасности, осуществляющие идентификацию и аутентификацию пользователей, управление доступом, межсетевое экранирование,аудит и мониторинг сети, управление удаленным доступом и т. д.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАЩИТА РЕСУРСОВ

РЕСУРСЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

объекты данных, которые связаны с системными сервисами или функциями; они включают системные программы и файлы, подсистемы и программные продукты.
Ресурсы операционной системы обычно находятся под управлением и ответственностью провайдера сервиса. Их целостность должна гарантироваться, поскольку эти данные критичны для того сервиса, который организация хочет поставлять.

РЕСУРСЫ ПОЛЬЗОВАТЕЛЕЙ

объекты данных, которые связаны с отдельными пользователями или группами пользователей. Ресурсы пользователей должны быть защищены в соответствии с требованиями собственника данных. Для гарантии хотя бы минимального уровня безопасности рекомендуется установить по умолчанию некоторую начальную защиту этих ресурсов.

ОПРЕДЕЛЕНИЕ АДМИНИСТРАТИВНЫХ ПОЛНОМОЧИЙ

полномочия системного администратора;

все действия, необходимые для управления компьютерными системами. Эти полномочия могут дать возможность администратору обойти контроль безопасности, но это должно рассматриваться как злоупотребление полномочиями

полномочия администратора безопасности

Возможность администратора выполнять действия, необходимые для управления безопасностью. Эти полномочия позволяют администратору осуществлять изменение системных компонентов или считывать конфиденциальные данные.

-определить для каждой системной платформы или системы управления доступом те полномочия, которые могут быть признаны в указанных категориях;
- назначить полномочия администраторам в соответствии с индивидуальной ответственностью;
- периодически проверять назначение идентификаторов авторизованным пользователям.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

РОЛИ И ОТВЕТСТВЕННОСТИ В БЕЗОПАСНОСТИ СЕТИ

провайдер сервисов предоставляет сервисы обработки информации

Аудитор отвечает за:
- исполнение политик безопасности;
– исполнение процессов безопасности;
– периодическое выполнение контрольной оценки безопасности;
– задание требований для приложений/инструментов/решений в целях обеспечения требуемой безопасности;

пользователь данными исполняет инструкций безопасности (пароль должен быть нетривиальным и удовлетворять утвержденным синтаксическим правилам и другие)

менеджер данных отвечает за управление безопасностью распределяемых данных (оценка уровня конфиденциальности данных с целью их классификации; установление определенного уровня защиты)

администратор безопасности отвечает за настройку и управление системных средств управления безопасностью (установка системных политик, включая парольную политику, управление атрибутами доступа пользователей, выполнение периодических проверок)

АУДИТ И ОПОВЕЩЕНИЕ

АУДИТ

способность регистрировать все важные, с точки зрения безопасности, действия, выполненные в компьютерной среде.

ОПОВЕЩЕНИЕ

способность оповещать об этих действиях в читабельной форме

ДВА АСПЕКТА АУДИТА

- **какие события особенно важны для безопасности** (все нарушения безопасности, такие как: неавторизованный доступ к системе неправильный пароль; аннулированный пароль; неавторизованный доступ к ресурсу; все попытки доступа к чувствительным/важным областям систем; все выдаваемые команды безопасности, использующие административные полномочия; все попытки доступа к ресурсам операционных систем, за исключением доступа по умолчанию.);
- **как долго должны храниться записи регистрации**

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТИПОВЫЕ НЕДОСТАТКИ В РЕАЛИЗАЦИИ ФУНКЦИЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

- Общие недостатки АБС и банковских приложений;
- Типовые недостатки приложений дистанционного банковского обслуживания и электронных средств платежа;
- Типовые недостатки веб-приложений;
- Типовые недостатки систем управления базами данных;
- Типовые недостатки операционных систем;
- Типовые недостатки телекоммуникационного оборудования;
- Типовые недостатки технологий виртуализации

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ НЕДОСТАТКИ АБС И БАНКОВСКИХ ПРИЛОЖЕНИЙ

УПРАВЛЕНИЕ ДОСТУПОМ

Отсутствие ограничений на количество одновременных подключений (сессий) пользователя в АБС. Упрощает использование нарушителями учетных записей, принадлежащих сотрудникам организации БС РФ

РЕГИСТРАЦИЯ СОБЫТИЙ И ПРОСМОТР ЖУРНАЛОВ РЕГИСТРАЦИИ СОБЫТИЙ

Наличие в данных журналов регистрации событий конфиденциальных и чувствительных данных (пароли пользователей, данные платежных карт и т.п.)

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Использование процедур самостоятельного восстановления или смены забытых пользователями паролей.

Отсутствие предварительной аутентификации при смене пароля пользователем.

ЗАЩИТА ДАННЫХ

Отсутствие в АБС механизмов очистки остаточной информации при удалении данных

КОНФИГУРАЦИЯ БЕЗОПАСНОСТИ

Отсутствие механизмов защиты от несанкционированного доступа к настройкам приложения

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТИПОВЫЕ НЕДОСТАТКИ ПРИЛОЖЕНИЙ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ И ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

- Использование однофакторной аутентификации при выполнении финансовых операций;
- Предсказуемый алгоритм формирования однократных паролей и (или) возможность повторного использования однократных паролей

БЕЗОПАСНОСТЬ ТРАНЗАКЦИЙ

- Использование для подтверждения транзакций средств авторизации, допускающих возможность формирования подтверждения третьими лицами;
- использование для формирования электронной цифровой подписи ключевых носителей, допускающих экспорт закрытой части ключа подписи;
- отсутствие возможности подписания электронных платежных поручений юридических лиц электронными подписями двух уполномоченных лиц;
- возможность повторного использования электронного платежного документа;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТИПОВЫЕ НЕДОСТАТКИ ВЕБ-ПРИЛОЖЕНИЙ

РАЗМЕЩЕНИЕ КОМПОНЕНТОВ ВЕБ-ПРИЛОЖЕНИЯ

-Совместное расположение журналов регистрации событий и системных файлов;

-Наличие на веб-сервере тестовых приложений и сценариев, а также программных компонентов, не входящих в состав АБС.

ЗАЩИТА ДАННЫХ

-Отсутствие в параметрах веб-формы, предназначенных для ввода конфиденциальной информации, директив, запрещающих кеширование данных.

-Передача конфиденциальной и аутентификационной информации в сообщениях HTTP-GET

УПРАВЛЕНИЕ СЕССИЯМИ

-Использование предсказуемых идентификаторов сессий.

-Возможность повторного использования идентификатора сессии (в том числе использование одинаковых идентификаторов в нескольких сессиях одного пользователя, неизменность идентификатора сессии после повторной аутентификации пользователя).

- Возможность использования идентификатора сессии после ее завершения

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТИПОВЫЕ НЕДОСТАТКИ ОПЕРАЦИОННЫХ СИСТЕМ

УПРАВЛЕНИЕ ДОСТУПОМ

-Отсутствие ограничений по составу пользователей, имеющих право удаленного доступа к операционной системе, и IP-адресам, с которых разрешен такой доступ.

-Использование незащищенных и слабозащищенных протоколов удаленного доступа к операционной системе (например, TELNET, PPTP).

УПРАВЛЕНИЕ СИСТЕМОЙ

Отключение в настройках ядра операционной системы функции очистки файла/ раздела подкачки виртуальной памяти. 5.3.3. Включенная в настройках операционной системы возможность выгрузки образов областей памяти (дампов) на диск

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

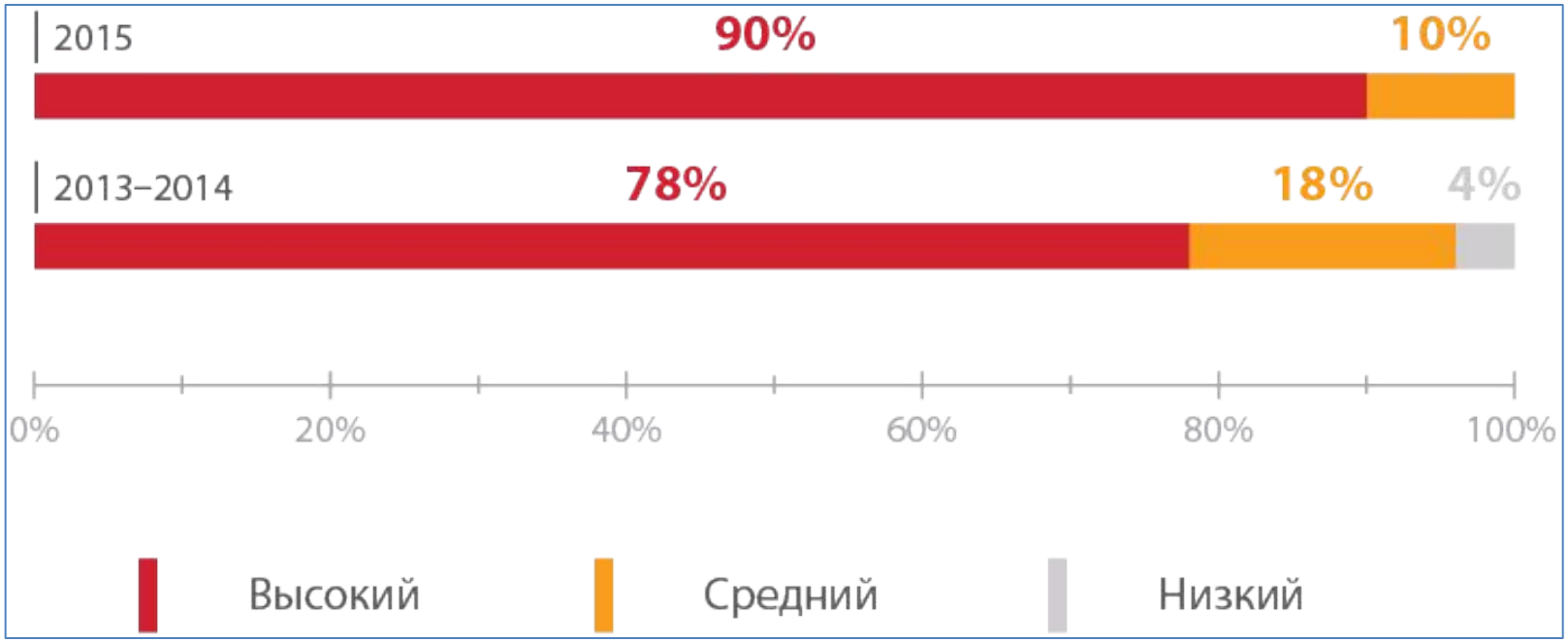
-Отображение на приглашении для входа в систему сведений, на основе которых могут быть установлены имена пользователей операционной системы или получены какие-ли- бо сведения о паролях пользователей.

-Возможность доступа к операционной системе без аутентификации через вспомо-гательные и (или) редко используемые интерфейсы (serial-порты и т.п.).

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

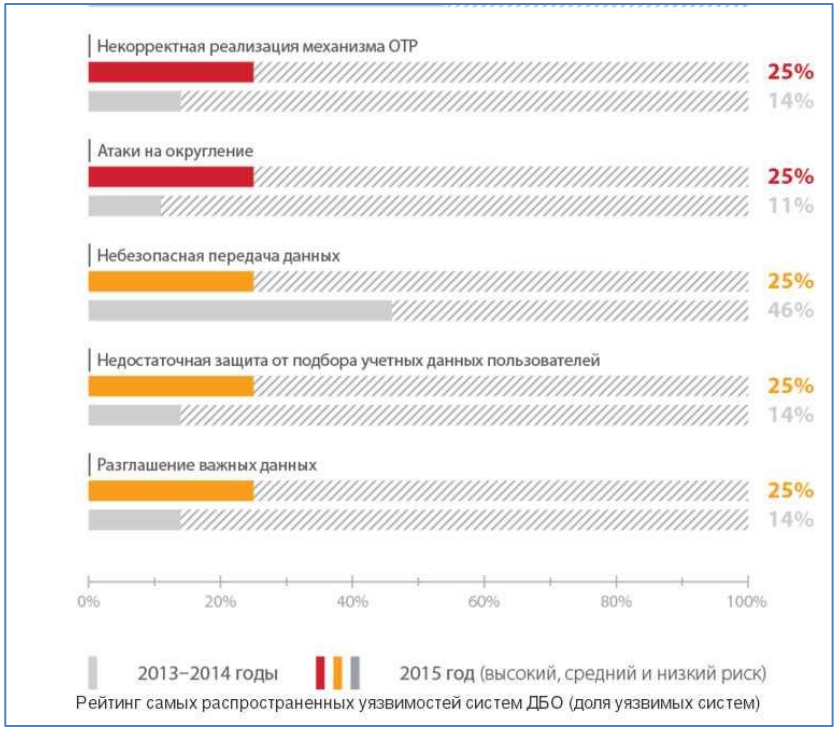
УЯЗВИМОСТИ ОНЛАЙН-БАНКОВ 2016

Распределение систем по максимальной степени риска обнаруженных уязвимостей



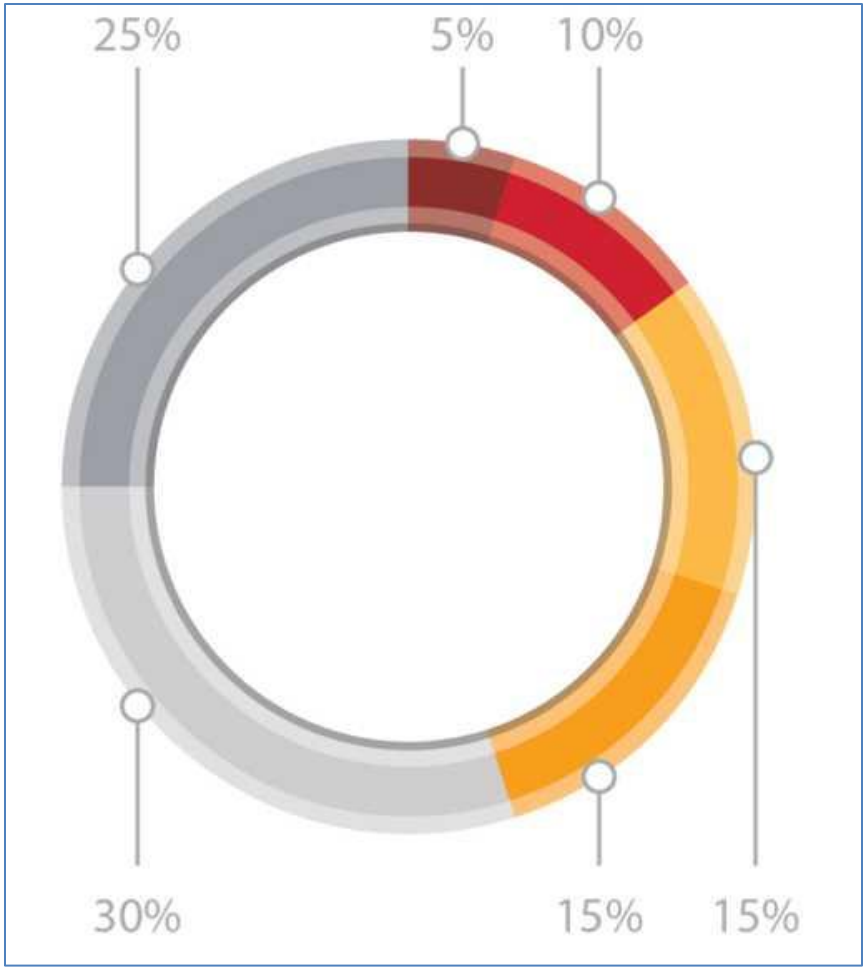
РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЕЙТИНГ САМЫХ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ СИСТЕМ ДБО (ДОЛЯ УЯЗВИМЫХ СИСТЕМ)



Рейтинг самых распространенных уязвимостей систем ДБО (доля уязвимых систем)

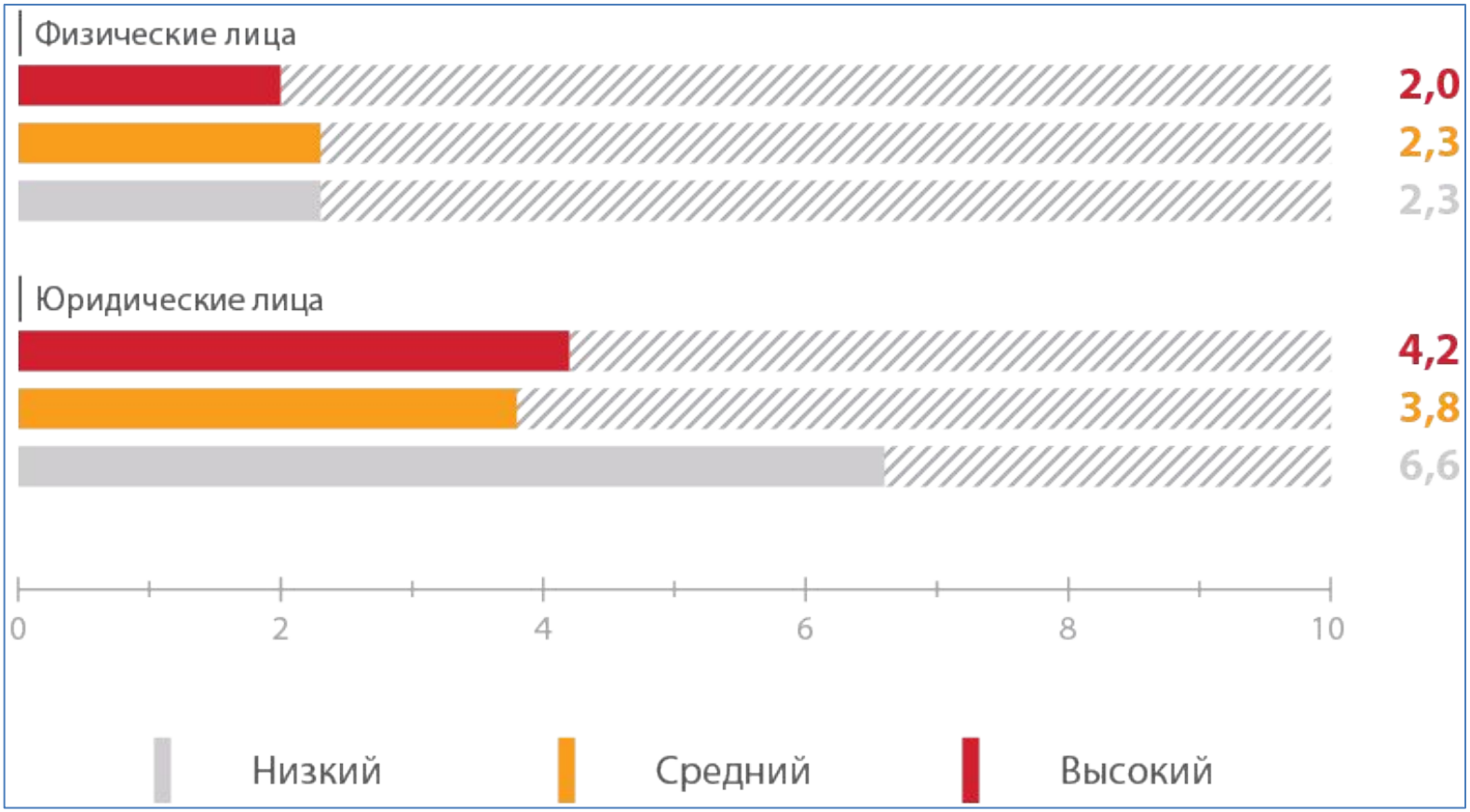
Реализуемые угрозы информационной безопасности систем ДБО



- Кража денежных средств со стороны внешнего злоумышленника
- Кража денежных средств со стороны авторизованного пользователя, доступ к ОС или СУБД
- Кража денежных средств со стороны авторизованного пользователя, несанкционированный доступ к банковской тайне
- Доступ к СУБД или файловой системе, несанкционированный доступ к банковской тайне
- Доступ к файловой системе или СУБД
- Несанкционированный доступ к сведениям, составляющим банковскую тайну на уровне отдельных клиентов

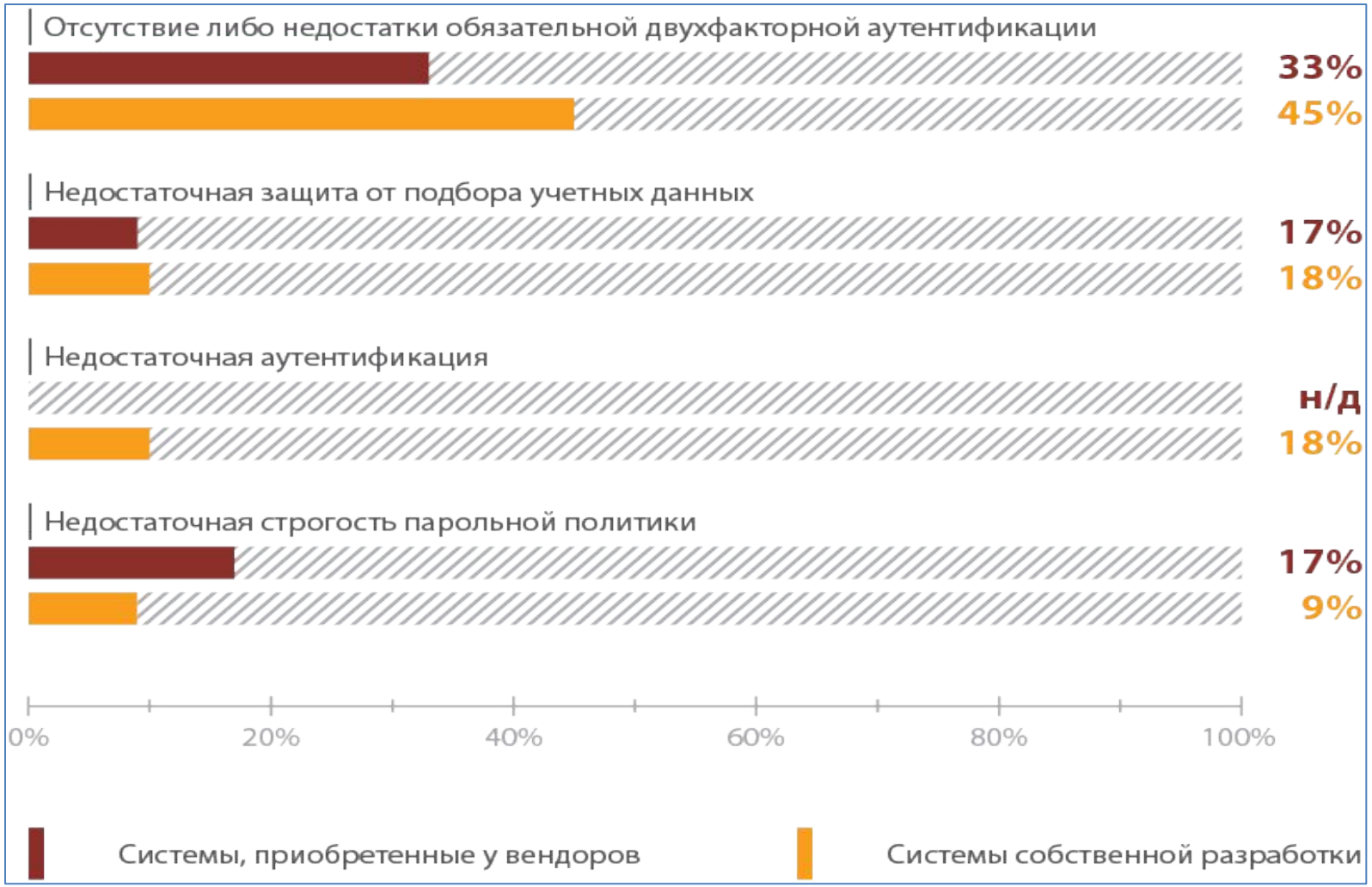
РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПРЕДЕЛЕНИЕ ПО СУБЪЕКТАМ



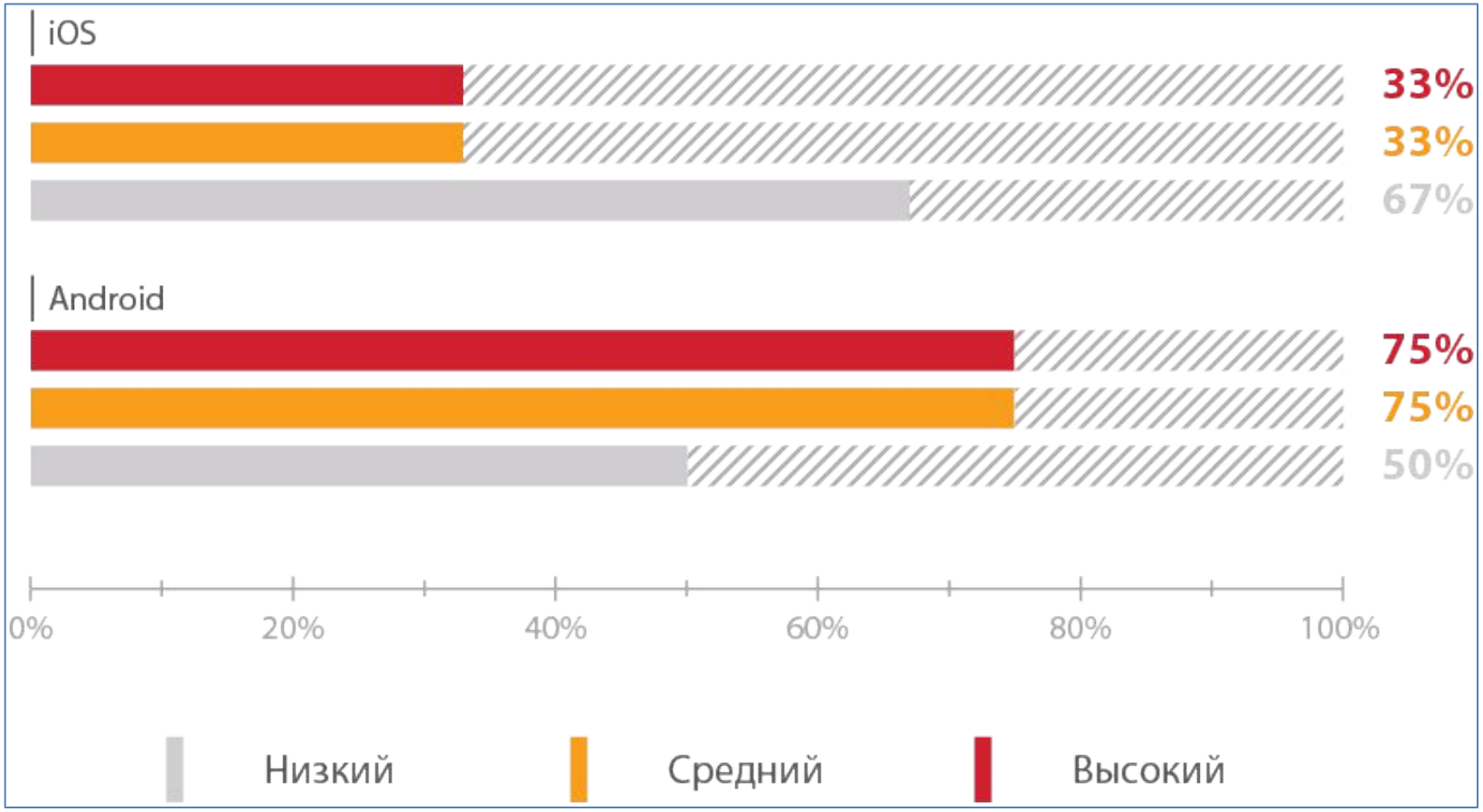
РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Доля систем, подверженных уязвимостям механизмов аутентификации (для различных категорий разработчиков)



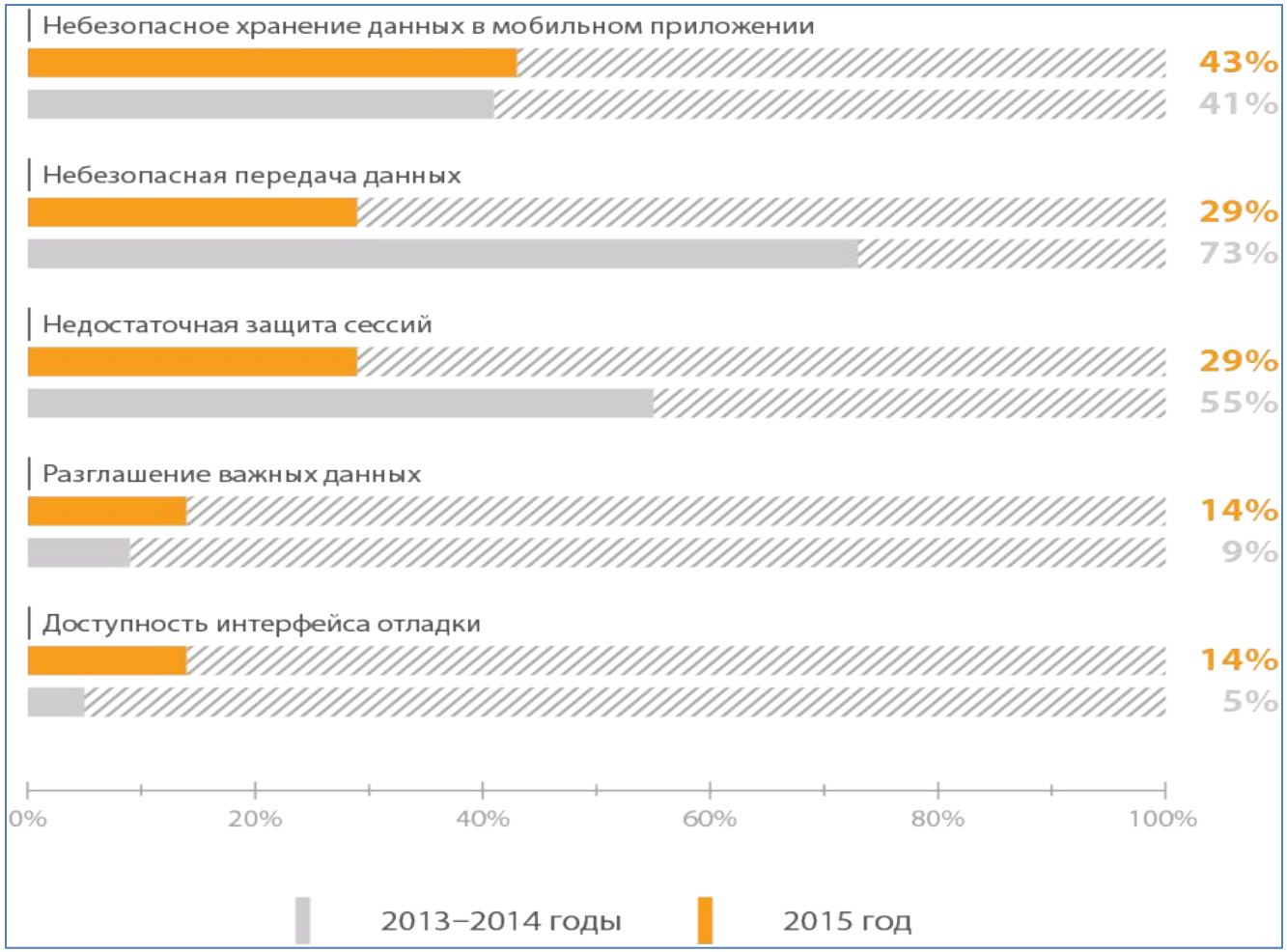
РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Мобильные системы ДБО



РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Наиболее распространенные уязвимости клиентского ПО мобильных систем



РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫВОДЫ

- Уровень защищенности систем ДБО остается низким, несмотря на сокращение общей доли критически опасных уязвимостей среди всех выявленных недостатков по сравнению с прошлыми годами.
- Низкая защищенность систем ДБО, находящихся в эксплуатации, наглядно свидетельствует о необходимости внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений.
- Анализ защищенности систем необходимо проводить не только на этапах разработки приложения и перед вводом системы в эксплуатацию, но и во время ее активного использования клиентами банка. Причем такой анализ необходимо осуществлять на регулярной основе (например, дважды в год) с контролем устранения выявленных недостатков.
- Системам ДБО, приобретенным у вендоров, стоит уделить особое внимание: они зачастую более подвержены уязвимостям, чем системы собственной разработки банков. Кроме того, рекомендуется использовать средства превентивной защиты, такие как межсетевой экран уровня приложения.
- Для получения доступа к личному кабинету пользователя нарушителю достаточно использовать давно известные и распространенные уязвимости (например, недостаточную защиту сессии).

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОМАШНЕЕ ЗАДАНИЕ

Задание: Подготовьте реферат о вредоносном программном обеспечении, включив в него следующие разделы:

- Тип и содержание вредоносного программного обеспечения
- Используемые уязвимости и угрозы данного программного обеспечения
- Статистика (число атакованных пользователей, кража денежных средств и т.д.), распространение и перспективы развития
- Предложения по профилактике и удалению данного зловредного ПО

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОКЛАДЫ

1	Conficker
2	Tinba
3	Sality
4	Gozi
5	Petya
6	Gootkit
7	Zeus
8	Angler EK
9	Teslacrypt
10	CoreBot
11	Cutwail
12	Dridex
13	Adwind

14	Nemesis
15	DressCode
16	Carbanak
17	QAKBOT
18	GM Bot
19	Dyreza
20	Citadel
21	GozNym
22	Tordow
23	Marcher
24	ZBot

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СПАСИБО ЗА ВНИМАНИЕ!

Информационная безопасность