РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.6-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Дата введения: 2014-09-01

Москва
2014

Предисловие

ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 10 июля 2014 года № Р-556.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) организациям банковской системы Российской Федерации (БС РФ) требуется принимать меры к обеспечению информационной безопасности (ИБ) автоматизированных банковских систем (АБС) на всех стадиях их жизненного цикла.

Принятие мер к обеспечению ИБ на стадиях жизненного цикла АБС осуществляется с целью выполнения следующих основных задач:

— обеспечение реализации в АБС необходимых требований к обеспечению ИБ, установленных законодательством Российской Федерации, в том числе нормативными актами Банка России, СТО БР ИББС-1.0, внутренними документами организации БС РФ;
— снижение рисков нарушения ИБ, связанных с наличием уязвимостей в АБС;
— контроль обеспечения ИБ в рамках эксплуатации АБС;
— снижение рисков нарушения ИБ, в том числе рисков утечки информации, на этапе сопровождения, модернизации АБС и вывода из эксплуатации АБС;
— оперативная модернизация АБС в случае выявления недопустимых рисков нарушения ИБ, связанных с ее эксплуатацией.

С целью установления рекомендаций по выполнению указанных задач настоящий документ устанавливает положения:

— по организации работ на этапах жизненного цикла АБС, в том числе обеспечивающей возможность контроля с целью установления доверия к проведению указанных работ и, соответственно, доверия к реализации обеспечения ИБ в АБС;
— по составу типовых недостатков в реализации требований к обеспечению ИБ в АБС, создающих условия для возникновения недопустимых рисков нарушения ИБ при эксплуатации АБС (далее – типовые недостатки в обеспечении ИБ АБС);
— по составу, содержанию и порядку проведения работ по контролю исходного кода программного обеспечения АБС, оценке защищенности АБС и по контролю параметров настроек технических защитных мер (выявление ошибок конфигурации).

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Дата введения: 2014-09-01

1. Область применения

Настоящие рекомендации распространяются на организации БС РФ, реализующие требования СТО БР ИББС-1.0 по обеспечению ИБ на этапах жизненного цикла АБС в рамках построения (совершенствования) системы обеспечения ИБ, а также на организации, привлекаемые организациями БС РФ для выполнения работ на стадиях жизненного цикла АБС.

Настоящий документ применяется в организациях БС РФ и иных организациях путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах и договорах, заключаемых организацией БС РФ.

Рекомендательный статус документа допускает, что по решению организации БС РФ вместо его отдельных положений могут применяться иные положения, обеспечивающие эквивалентный (аналогичный) уровень обеспечения ИБ в АБС на различных стадиях их жизненного цикла.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на следующие документы:

СТО БР ИББС-1.0;

Рекомендации в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ” (РС БР ИББС-2.2).

3. Термины и определения

В настоящих рекомендациях применяются термины в соответствии со СТО БР ИББС-1.0, а также следующие термины с соответствующими определениями:

3.1. **Доверие** — состояние уверенности в том, что АБС соответствует установленным для нее требованиям к обеспечению ИБ.

3.2. **Функция обеспечения ИБ** — реализованная функциональная возможность одного или нескольких компонентов АБС, связанная с обеспечением ИБ.

3.3. **Интерфейс (использования) функции обеспечения ИБ** — описание и реализация способов использования функций обеспечения ИБ.

3.4. **Функциональные требования к обеспечению ИБ** — требования к функциям обеспечения ИБ компонентов АБС, а также интерфейсам их использования.

4. Обозначения и сокращения

АБС — автоматизированная банковская система
АРМ — автоматизированное рабочее место
СУБД — система управления базами данных
ТЗ — техническое задание
ЧТЗ — частное техническое задание
ИБ — информационная безопасность
БС РФ — банковская система Российской Федерации

5. Общие положения

5.1. В рамках настоящих рекомендаций АБС рассматривается как взаимосвязанная совокупность программно-технических средств: телекоммуникационного оборудования, средств вычислительной техники, системного программного обеспечения, прикладного программного обеспечения, а также средств защиты информации.

Основные функциональные возможности АБС, обеспечивающие автоматизацию банковских информационных и платежных технологических процессов, в том числе существенные защитные меры, реализуются одним или несколькими специализированными банковскими приложениями, входящими в состав АБС. Остальные компоненты, в том числе системное программное обеспечение, средства вычислительной техники, средства защиты информации, рассматриваются как обеспечивающая среда функционирования специализированных банковских приложений (далее — обеспечивающие компоненты АБС).

5.2. Обеспечение ИБ в АБС реализуется использованием функций обеспечения ИБ компонентов АБС, которое заключается в применении и эксплуатации защитных мер специализированных банковских приложений, а также защитных мер всех обеспечивающих компонентов АБС. Совокупность защитных мер специализированных банковских приложений АБС и защитных мер всех обеспечивающих компонентов АБС определяется как подсистема ИБ АБС.

Следует учитывать, что обеспечивающие компоненты АБС могут использоваться для обеспечения эксплуатации нескольких разных специализированных банковских приложений, соответственно, функции обеспечения ИБ таких обеспечивающих компонентов могут использоваться в разных АБС, а их защитные меры включаются в подсистемы ИБ разных АБС.

5.3. С учетом того, что обеспечивающие компоненты АБС могут являться объектом целенаправленных действий со стороны злоумышленника, обеспечение ИБ на этапах жизненного цикла АБС требует реализации мероприятий как для специализированных банковских приложений, так и для всех обеспечивающих компонентов АБС.

При организации работ на стадиях жизненного цикла АБС рекомендуется учитывать, что в ряде случаев обеспечивающие компоненты АБС создаются разными организациями, большая их часть поставляется как есть и организация — разработчик специализированных банковских приложений (далее — разработчик) не располагает полной и достоверной информацией о корректности реализации функций безопасности обеспечивающих компонентов АБС.

5.4. В соответствии с требованиями СТО БР ИББС-1.0 жизненный цикл АБС разделяется на следующие стадии:

1) разработка технического задания (ТЗ);
2) проектирование;
3) создание и тестирование;
4) приемка и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

5.5. Доверие к реализации обеспечения ИБ в АБС возможно только при наличии определенных свидетельств полноты и корректности проведения мероприятий по обеспечению ИБ на стадиях жизненного цикла компонентов АБС, как минимум специализированных банковских приложений. В качестве свидетельств доверия рекомендуется рассматривать:

— регламенты, используемые для организации деятельности по обеспечению ИБ на этапах жизненного цикла АБС;
— документированные результаты выполнения деятельности по обеспечению ИБ на этапах жизненного цикла АБС.

На каждой стадии жизненного цикла формируется собственный набор свидетельств доверия, по результатам оценки которых может быть принято решение о полноте и корректности реализации требований к обеспечению ИБ, предъявляемых к АБС.

5.6. Организацию работ по созданию АБС, включая подсистему ИБ, рекомендуется осуществлять с учетом положений комплекса стандартов и руководящих документов на автоматизированные системы “Информационная технология”, в том числе ГОСТ 34.601-90 “Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания” (далее — ГОСТ 34.601-90).

6. Стадия разработки технического задания

6.1. Основной задачей на стадии разработки ТЗ в части обеспечения ИБ является определение требований к обеспечению ИБ для создаваемой АБС для включения в состав ТЗ (далее — требования ТЗ к обеспечению ИБ).

Следует учитывать, что на данной стадии, как правило, отсутствует полная информация, необходимая для установления конкретных функциональных требований к обеспечению ИБ, реализуемых компонентами АБС. Установление конкретных функциональных требований к обеспечению ИБ возможно только после того, как будут определены основные технические решения создаваемой АБС. В связи с этим требования ТЗ к обеспечению ИБ рекомендуется формулировать в общем (неявном) виде, без привязки к конкретным реализациям, но при этом требования должны быть четко определены в объеме, достаточном для их однозначного понимания.

6.2. Формирование требований ТЗ к обеспечению ИБ рекомендуется осуществлять с учетом положений ГОСТ 34.602-89 “Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы”.

6.3. Требования ТЗ к обеспечению ИБ определяются (составляются) на основе требований к обеспечению ИБ, установленных законодательством Российской Федерации, в том числе нормативными актами Банка России, СТО БР ИББС-1.0, внутренними документами организации БС РФ, которые должны быть реализованы для создаваемой АБС.

Определение состава документов, требования к обеспечению ИБ которых используются для формирования ТЗ к обеспечению ИБ, рекомендуется осуществлять на основе данных:

- о типах информации (информационных активов), предполагаемых к обработке и (или) хранению в АБС;
- о составе банковских технологических процессов организации БС РФ, для автоматизации которых она создается;
- о технологиях и средствах обработки информации, предполагаемых к использованию для реализации АБС (в случае наличия подобных данных).

6.4. При определении требований ТЗ к обеспечению ИБ рекомендуется установить:

- необходимость и целесообразность применения средств защиты информации, сертифицированных по требованиям безопасности информации;
- необходимость и целесообразность привлечения для проведения работ по созданию, модернизации, эксплуатации и выводу из эксплуатации АБС организации, имеющей лицензии на деятельность по технической защите конфиденциальной информации.

6.5. При формировании требований ТЗ к обеспечению ИБ дополнительно рекомендуется осуществить предварительный анализ актуальных угроз безопасности информации. На данном этапе рекомендуется формулировать угрозы ИБ в самом общем виде в терминах бизнес-процессов, операций и функций организации БС РФ.

В случае если на данной стадии могут быть сформированы функциональные требования к обеспечению ИБ по нейтрализации рассмотренных актуальных угроз или компенсации возможного ущерба, рекомендуется включить указанные требования в состав ТЗ к обеспечению ИБ.

6.6. В состав требований ТЗ к обеспечению ИБ рекомендуется включать требования к использованию функций обеспечения ИБ обеспечивающих компонентов АБС, используемых для обеспечения ИБ специализированных банковских приложений разных АБС, со стороны специализированных банковских приложений (требования к интеграции специализированных банковских приложений с разделяемыми обеспечивающими компонентами АБС).

6.7. Среди прочего в состав требований ТЗ к обеспечению ИБ рекомендуется включать:

- требования к обеспечению ИБ, связанные с назначением и распределением ролей в АБС;
- требования к обеспечению ИБ, связанные с управлением доступом и регистрацией;
- требования к обеспечению ИБ, связанные с защитой от воздействия вредоносного кода;
- требования к обеспечению ИБ, связанные с использованием общедоступных сетей и каналов передачи данных;
- требования к обеспечению ИБ, связанные с использованием средств криптографической защиты информации;

— требования к обеспечению ИБ, связанные с реализацией контроля эксплуатации применяемых защитных мер;
— требования к обеспечению ИБ, связанные с реализацией мониторинга ИБ, в том числе для выявления инцидентов ИБ в АБС;
— требования к безопасным технологиям обработки информации (технологическим мерам защиты информации).

6.8. ТЗ на создаваемую АБС рекомендуется как основной источник требований к обеспечению ИБ на стадии проектирования АБС.

7. Стадия проектирования АБС

7.1. Основными задачами на стадии проектирования АБС в части обеспечения ИБ являются:

— установление и документирование функциональных требований, реализуемых компонентами АБС, обеспечивающих выполнение требований ТЗ к обеспечению ИБ;
— определение состава функций обеспечения ИБ, реализуемых разделяемыми обеспечивающими компонентами АБС;
— выбор состава защитных мер (технических и (или) организационных), реализующих функции обеспечения ИБ в соответствии с функциональными требованиями к обеспечению ИБ в привязке к компонентам АБС, в том числе выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации;
— первичное определение параметров настройки технических защитных мер (стандартов конфигураций);
— определение и документирование интерфейсов использования функций обеспечения ИБ, реализованных в компонентах АБС;
— первичное определение правил эксплуатации технических защитных мер, включая правила их обновления, управления и контроля параметров их настройки;
— определение требований (состав и содержание) к регламентам реализации организационных защитных мер;
— первичное определение состава ролей субъектов доступа АБС (эксплуатирующего персонала, пользователей, программных процессов), состав ресурсов доступа (баз данных, файловых ресурсов, виртуальных машин, иных ресурсов доступа), прав доступа ролей субъектов доступа (чтение, запись, выполнение или иные типы доступа) при осуществлении доступа к ресурсам доступа;
— первичное определение требований к кадровому обеспечению подсистемы ИБ АБС.

7.2. Проектирование АБС в части обеспечения ИБ рекомендуется начинать с разработки архитектуры подсистемы ИБ АБС, в которую рекомендуется включать описание:

— предполагаемой реализации требований ТЗ к обеспечению ИБ компонентами проектируемой АБС;
— предполагаемого использования функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС;
— предполагаемого взаимодействия компонентов АБС для обеспечения ИБ в АБС.

Разработку архитектуры АБС для обеспечения ИБ следует осуществлять на основе:

— данных о разделении АБС на компоненты, составе и функциях специализированных банковских приложений и обеспечивающих компонентов АБС;
— идентификации (для стандартных) или описания (для разрабатываемых в составе АБС или самостоятельно разрабатываемых) интерфейсов взаимодействия между компонентами АБС;
— данных о программном обеспечении АБС, в том числе системном, которое является покупным коробочным (для АБС, создаваемых путем адаптации специализированного прикладного обеспечения, — данные о пакетах специализированных прикладных программ).

7.3. Проектирование подсистемы ИБ АБС рекомендуется выполнять с учетом целесообразности реализации:

— централизованного управления и контроля технических защитных мер, в том числе в части обновления программного обеспечения, обновления применяемых сигнатурных баз, установления и контроля параметров их настройки;
— интеграции АБС с инфраструктурными компонентами мониторинга ИБ и выявления инцидентов ИБ, применяемыми в организации БС РФ, для чего в состав функциональных требований к обеспечению ИБ рекомендуется включить требования к составу данных мониторинга ИБ, генерируемых компонентами АБС в процессе эксплуатации АБС;

— максимально возможной степени использования функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС.

При проектировании подсистемы ИБ АБС не рекомендуется планировать необоснованную модернизацию эксплуатируемых разделяемых обеспечивающих компонентов АБС. В случае проведения модернизации указанных компонентов рекомендуется организация и проведение работ по модернизации и тестированию в части обеспечения ИБ всех АБС, использующих разделяемый обеспечивающий компонент, подвергшийся модернизации.

7.4. На этапе проектирования рекомендуется установить функциональные требования к обеспечению ИБ, включая:

— функциональные требования к обеспечению ИБ специализированных банковских приложений;
— функциональные требования к обеспечению ИБ обеспечивающих компонентов разрабатываемой АБС;
— требования к использованию функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС.

Функциональные требования к обеспечению ИБ рекомендуется документировать в частном ТЗ на АБС (далее — ЧТЗ подсистемы ИБ АБС).

Если функциональные требования к обеспечению ИБ установлены на стадии разработки ТЗ, их повторное документирование в ЧТЗ подсистем ИБ АБС нецелесообразно.

7.5. С целью обеспечения полноты реализации требований ТЗ к обеспечению ИБ рекомендуется выполнять процедуры контроля соответствия требований ТЗ к обеспечению ИБ и функциональных требований к обеспечению ИБ, включенных в ЧТЗ подсистемы ИБ.

Функциональные требования ЧТЗ подсистемы ИБ АБС рекомендуется разделять на категории с учетом выполнения пункта 7.4 настоящего документа и документировать в отдельных подразделах ЧТЗ подсистемы ИБ АБС.

В случаях, когда к различным составным частям АБС предъявляются одинаковые функциональные требования, рекомендуется дублировать их в соответствующих подразделах ЧТЗ подсистемы ИБ АБС.

7.6. Функциональные требования ЧТЗ подсистемы ИБ АБС рекомендуется рассматривать в качестве основного документа, на соответствие которому оцениваются свидетельства доверия, формируемые на последующих стадиях жизненного цикла АБС.

7.7. При проектировании подсистемы ИБ АБС рекомендуется определение и оформление стандартов конфигурации — документов, содержащих перечень и эталонные значения конфигурационных параметров компонентов АБС, в том числе технических защитных мер. Принятие стандартов конфигурации и контроль соответствия фактических значений параметров конфигурации их эталонным значениям — основной способ предотвращения уязвимостей, вызванных ошибками настройки компонентов АБС.

С целью формирования стандартов конфигурации обеспечивающих компонентов АБС, являющихся серийно выпускаемым программным обеспечением, в том числе операционными системами, системами управления базами данных, иным системным программным обеспечением, рекомендуется использовать стандартизованные справочники параметров конфигураций в части обеспечения ИБ, например National Checklist Program Repository [1].

7.8. Для АБС, компоненты которых предполагается размещать на средствах вычислительной техники клиентов организации БС РФ, рекомендуется определение и документирование:

— состава компонентов, передаваемых на сторону клиента;
— мер, принимаемых для обеспечения целостности программных компонентов, передаваемых на сторону клиента;
— требований к среде функционирования компонентов АБС на стороне клиента;
— требований и порядка передачи клиентом информации о проблемах и инцидентах ИБ, возникших при использовании клиентом компонентов АБС;
— требований и способов обновления компонентов АБС, эксплуатируемых на стороне клиента, а также требований к обновлению среды их функционирования.

7.9. На этапе разработки технического проекта разрабатывается проектная документация, включающая в себя проектную документацию на подсистему ИБ АБС. Определение состава и структуры проектной документации АБС рекомендуется осуществлять с учетом положений руководящего документа РД 50-34.698-90 “Автоматизированные системы. Требования к содержанию документов”, а также ГОСТ 34.201-89 “Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем” и ГОСТ 19.201-78 “Единая система программной документации. Техническое задание. Требования к содержанию и оформлению”.

7.10. Проектную документацию подсистемы ИБ АБС рекомендуется разрабатывать с соблюдением следующих принципов:

— проектная документация должна содержать документированные результаты выполнения задач, установленных в пункте 7.1 настоящего документа;
— проектная документация должна предоставлять возможность проведения контроля полноты и корректности реализации функций обеспечения ИБ в соответствии с требованиями ЧТЗ подсистемы ИБ АБС в реализованных проектных решениях.

8. Стадия создания и тестирования АБС

8.1. Основными задачами на стадии создания и тестирования АБС в части обеспечения ИБ являются:

— управление версиями и изменениями разрабатываемых специализированных банковских приложений;
— обеспечение ИБ среды разработки и тестирования компонентов АБС;
— тестирование (проведение предварительных испытаний) компонентов АБС, в том числе специализированных банковских приложений;
— тестирование (проведение предварительных испытаний) компонентов АБС, предназначенных для эксплуатации на средствах вычислительной техники клиентов организации БС РФ;
— разработка эксплуатационной документации.

8.2. Основными рекомендуемыми целями применения управления версиями и изменениями разрабатываемых программных компонентов АБС в части обеспечения ИБ являются:

— контроль соответствия реализации определенных требований ЧТЗ на подсистему ИБ АБС в определенной версии (сборке) разрабатываемых специализированных банковских приложений;
— формализация порядка хранения исходных файлов и работы с ними, а также принятие мер, препятствующих несанкционированному внесению изменений в версии специализированных банковских приложений.

8.3. Для обеспечения управления версиями и изменениями разрабатываемых специализированных банковских приложений рекомендуется использовать систему управления версиями и изменениями, позволяющую осуществлять:

— маркировку (присвоение номеров) промежуточных версий разрабатываемых специализированных банковских приложений;
— идентификацию исходных файлов, используемых для сборки каждой промежуточной версии разрабатываемых специализированных банковских приложений, в том числе файлов исходного кода, ресурсных файлов, файлов документации;
— маркировку версий (редакций) исходных файлов.

8.4. Для обеспечения ИБ среды разработки и тестирования компонентов АБС рекомендуется обеспечить защиту от следующих угроз ИБ:

— несанкционированное внесение изменений в исходные файлы разрабатываемого программного обеспечения;
— приостановка процесса разработки и тестирования, приводящая к нарушению сроков выпуска окончательной (финальной) разрабатываемой версии программного обеспечения, в том числе вследствие нарушения работоспособности средств разработки, уничтожения части исходных файлов;
— несанкционированное ознакомление третьих лиц с исходными файлами и программной документацией, а также иная утечка информации в процессе разработки компонентов АБС;
— утрата прав (лицензий) на использование средств разработки.

Для противодействия угрозам разработчикам рекомендуется принять и документировать меры защиты, включающие:

— обеспечение контроля физического доступа к средствам вычислительной техники, используемым на стадии разработки и тестирования программных компонентов АБС;
— выделение сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые на стадии разработки специализированных банковских приложений;
— выделение сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые на стадии тестирования специализированных банковских приложений и обеспечивающих компонентов АБС;

— организацию и контроль изоляции и информационного взаимодействия сегмента разработки, сегмента тестирования и сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые для реализации банковских технологических процессов;
— управление доступом к ресурсам, средствам разработки и тестирования специализированных банковских приложений, в том числе исходным файлам;
— регистрацию и контроль действий с исходными файлами специализированных банковских приложений;
— организацию антивирусной защиты;
— контроль использования коммуникационных портов средств вычислительной техники.

8.5. В среде разработки и тестирования не рекомендуется использование реальных данных, полученных в результате реализации банковских технологических процессов.

В случае если для тестирования необходимы данные, максимально приближенные к реальным, рекомендуется формирование тестовых массивов данных путем необратимого обезличивания, маскирования и (или) искажения сведений, полученных в результате реализации банковских технологических процессов. Не рекомендуется использование в тестировании каких-либо данных, в отношении которых на основании законодательства Российской Федерации, в том числе нормативных актов Банка России, внутренних документов организации БС РФ и (или) договоров с клиентами и контрагентами, распространяется требование к обеспечению ИБ.

8.6. Тестирование полноты и корректности реализации требований ЧТЗ на подсистему ИБ АБС рекомендуется проводить в три стадии:
— непосредственно в ходе разработки программных компонентов АБС;
— перед выпуском финальной версии разрабатываемых программных компонентов АБС;
— в ходе предварительных испытаний АБС.

8.7. В ходе тестирования в рамках разработки специализированных банковских приложений рекомендуется проводить автономную проверку корректности реализации требований ЧТЗ подсистемы ИБ АБС к разрабатываемым специализированным банковским приложениям. Взаимодействие разрабатываемых специализированных банковских приложений с обеспечивающими компонентами АБС и их функциями обеспечения ИБ при этом, как правило, не тестируется, а сами обеспечивающие функции эмулируются с помощью тест-программ. Данное тестирование рекомендуется проводить разработчиками в среде разработки специализированных банковских приложений.

8.8. Перед выпуском финальной версии специализированных банковских приложений рекомендуется проводить тестирование полноты и корректности выполнения требований ЧТЗ на подсистему ИБ АБС к разрабатываемым специализированным банковским приложениям с учетом взаимодействия с обеспечивающими компонентами АБС, в том числе разделяемыми. Данное тестирование рекомендуется проводить разработчикам в тестовой среде, включающей в себя все компоненты АБС, размещенные и настроенные в соответствии с проектной документацией, и воспроизводящей близкие к реальным условия их эксплуатации.

8.9. Для тестирования разрабатываемых специализированных банковских приложений рекомендуется разработать и поддерживать в актуальном состоянии программу тестирования, включающую в себя проверку выполнения всех требований к обеспечению ИБ, установленных в ЧТЗ на подсистему ИБ АБС, в том числе при некорректных значениях входных данных, неработоспособности функций обеспечения ИБ прочих обеспечивающих компонентов АБС и иных возможных нештатных режимах функционирования АБС. Программа тестирования должна идентифицировать все тесты и демонстрировать соответствующими тестами полноту выполнения требований ЧТЗ на подсистему ИБ АБС.

Для каждого теста должна быть документирована методика тестирования, составляемая на основе информации об интерфейсах функций обеспечения ИБ, включающая исходные данные, последовательность проверочных действий, ожидаемый результат выполнения теста и критерии успешного или неуспешного выполнения теста.

Факт выполнения теста должен подтверждаться протоколом тестирования, содержащим дату тестирования, указание на методику тестирования, использованные при выполнении теста исходные данные, полученный результат и решение об успешном или неуспешном выполнении теста.

К моменту выпуска финальной версии разрабатываемых программных компонентов АБС корректность реализации их функций безопасности должна подтверждаться протоколами тестирования, демонстрирующими успешное выполнение всех тестов, предусмотренных программой тестирования.

8.10. Для программных компонентов АБС, реализующих банковский платежный технологический процесс или предназначенных для обработки персональных данных или иной информации, в отношении которой законодательством Российской Федерации или решением организации БС РФ установлено требование об обеспечении безопасности, рекомендуется перед проведением предварительных испытаний осуществлять контроль исходного кода с целью выявления типовых ошибок программирования и иных дефектов, приводящих к возникновению уязвимостей.

Рекомендации к проведению контроля исходного кода приведены в приложении 2 к настоящему документу.

8.11. В ходе предварительных испытаний АБС рекомендуется проведение независимого или совместного с разработчиком полного тестирования с целью проверки полноты и корректности реализации всех требований ЧТЗ на подсистему ИБ АСБ применительно ко всем компонентам АБС. Предварительные испытания рекомендуется проводить в тестовой среде, включающей в себя все компоненты АБС, конфигурированные и настроенные в соответствии с проектной документацией, и воспроизводящей близкие к реальным условия их эксплуатации.

Предварительные испытания рекомендуется проводить в соответствии с программой и методикой испытаний, в которой для каждого интерфейса каждой функции обеспечения ИБ должны быть предусмотрены процедуры тестирования, соответствующие этому интерфейсу. Тестирование должно подтверждать корректность:

— реализации функции обеспечения ИБ при доступе к ней через тестируемый интерфейс;
— вызовов необходимых функций обеспечения ИБ компонентов АБС, в том числе разделяемых.

Тесты должны демонстрировать соответствие результатов выполнения функции обеспечения ИБ на заданных наборах исходных данных требованиям безопасности, заданным в ЧТЗ.

8.12. Проведение предварительных испытаний рекомендуется осуществлять с учетом положений стандарта ГОСТ 34.603-92 “Информационная технология. Виды испытаний автоматизированных систем”.

8.13. По результатам выполнения стадии создания и тестирования АБС рекомендуется провести необходимые корректировки проектной документации на АБС.

8.14. В состав эксплуатационной документации, включая инструкции эксплуатационного персонала, в том числе администратора ИБ АБС, рекомендуется включать следующие сведения:

— описание состава защитных мер в привязке к компонентам АБС;
— описание состава, требований к размещению, параметров настройки (стандартов конфигураций) технических защитных мер;
— описание правил эксплуатации технических защитных мер, включая правила их обновления, управления и контроля их эксплуатации, в том числе параметров их настройки;
— требования и регламенты реализации организационных защитных мер;
— требования к кадровому обеспечению подсистемы ИБ АБС, описание ролей и функций эксплуатирующего персонала;
— требования к составу и содержанию организационных мероприятий, необходимых к проведению для обеспечения развертывания и эксплуатации подсистемы ИБ АБС, в том числе мероприятий по назначению ролей эксплуатационного персонала, обучению, информированию и повышению осведомленности эксплуатационного персонала и пользователей;
— описание правил и процедур обеспечения информационной безопасности при снятии с эксплуатации АБС или по окончании обработки информации.

8.15. Для АБС, компоненты которых предполагается размещать на средствах вычислительной техники клиентов организации БС РФ, в состав эксплуатационной документации рекомендуется включение отдельных документов, предназначенных для регламентации эксплуатации компонентов АБС на стороне клиента:

— описание состава компонентов АБС, эксплуатируемых на стороне клиента;
— порядок реализации мер, принимаемых для обеспечения целостности специализированных банковских приложений и обеспечивающих компонентов АБС, передаваемых на сторону клиента;
— требования к составу, версиям и необходимым настройкам в части обеспечения ИБ программного обеспечения среды функционирования компонентов АБС на стороне клиента;
— порядок обновления компонентов АБС, эксплуатируемых на стороне клиента, а также требования к обновлению программных компонентов среды их функционирования;
— требования к составу, версиям, обновлению и настройкам технических защитных мер, применяемых на стороне клиента.

9. Стадия приемки и ввода в действие

9.1. Основными задачами на стадии приемки и ввода в действие в части обеспечения ИБ являются:

— контроль развертывания компонентов АБС в информационной инфраструктуре организации БС РФ, используемой для реализации банковских технологических процессов (далее — промышленная или производственная среда);
— проведение опытной эксплуатации;
— устранение недостатков в реализации требований ЧТЗ на подсистему ИБ АБС;
— проведение приемочных испытаний.

9.2. Для контроля развертывания компонентов АБС в промышленной среде рекомендуется:

— обеспечить контроль корректности версий и целостности специализированных банковских приложений при передаче из среды разработки и тестирования в промышленную среду;
— обеспечить контроль выполнения требований проектной и эксплуатационной документации в части размещения и установления параметров настройки технических защитных мер, реализации организационных защитных мер, определения и назначения ролей.

9.3. Опытную эксплуатацию АБС рекомендуется проводить с учетом положений ГОСТ 34.603-92.

9.4. В рамках проведения опытной эксплуатации в части обеспечения ИБ рекомендуется проведение проверки корректности функционирования подсистемы ИБ АБС в промышленной среде, а также проверки возможности реализации на этапе эксплуатации положений проектной и эксплуатационной документации в части:

— контроля эксплуатации технических защитных мер, включая правила их обновления, управления и контроля параметров их настройки;
— контроля реализации организационных защитных мер;
— требований к кадровому обеспечению подсистемы ИБ АБС.

9.5. Дополнительно в рамках проведения опытной эксплуатации рекомендуется проведение комплексной оценки защищенности, включающей проведение:

— тестирования на проникновение;
— выявления известных уязвимостей компонентов АБС.

Комплексную оценку защищенности рекомендуется проводить без уведомления персонала, задействованного в опытной эксплуатации АБС, что среди прочего позволит оценить готовность персонала к выполнению требований документов организации БС РФ в части реагирования на инциденты ИБ.

Рекомендации к проведению оценки защищенности приведены в приложении 3 к настоящему документу.

9.6. По результатам опытной эксплуатации рекомендуется:

— документально зафиксировать состав выявленных недостатков в реализации подсистемы ИБ АБС;
— по каждому недостатку провести оценку рисков и принять решение о возможности их устранения на стадии эксплуатации;
— составить планы устранения недостатков в реализации подсистемы ИБ АБС;
— провести мероприятия по устранению критичных с точки зрения обеспечения ИБ недостатков в реализации подсистемы ИБ АБС.

9.7. После устранения недостатков в реализации подсистемы ИБ АБС рекомендуется принятие решения о составе и необходимости проведения мероприятий по повторному тестированию и опытной эксплуатации АБС и (или) ее компонентов с учетом выполненных доработок и уровня критичности устраняемых недостатков.

9.8. По результатам опытной эксплуатации рекомендуется рассмотреть необходимость доработки проектной и (или) эксплуатационной документации и в случае необходимости выполнить такую доработку.

9.9. После устранения критичных недостатков в реализации подсистемы ИБ АБС, выявленных в ходе опытной эксплуатации, проводятся приемочные испытания. Определение состава и порядка проведения приемочных испытаний рекомендуется осуществлять с учетом положений ГОСТ 34.603-92.

9.10. Приемочные испытания проводятся на основе результатов предварительных испытаний, опытной эксплуатации и результатов устранения критических недостатков, выявленных на стадии опытной эксплуатации. Кроме того, в рамках приемочных испытаний могут проводиться выборочные мероприятия по тестированию функций обеспечения ИБ, предусмотренные к проведению в рамках предварительных испытаний.

10. Стадия эксплуатации

10.1. Основными задачами на стадии эксплуатации в части обеспечения ИБ являются:

— контроль состава, мест размещения и параметров настроек технических защитных мер;
— контроль выполнения правил эксплуатации технических защитных мер, включая правила обновления и управления;
— контроль выполнения регламентов реализации организационных защитных мер;
— контроль реализации мер, принимаемых для обеспечения целостности специализированных банковских приложений и обеспечивающих компонентов АБС, передаваемых на сторону клиента, а также доведения до клиентов необходимых документов, входящих в состав эксплуатационной документации;
— контроль соблюдения требований к кадровому обеспечению подсистемы ИБ АБС;
— контроль выполнения организационных мероприятий, необходимых для обеспечения эксплуатации подсистемы ИБ АБС, в том числе мероприятий по назначению ролей эксплуатационного персонала, обучению, информированию и повышению осведомленности эксплуатационного персонала и пользователей;
— контроль готовности эксплуатационного персонала к эксплуатации подсистемы ИБ АБС;
— контроль информирования пользователей о правилах эксплуатации подсистемы ИБ АБС;
— периодическая оценка защищенности АБС (проведение мероприятий по выявлению типичных уязвимостей программных компонентов АБС, тестирование на проникновение);
— мониторинг сообщений об уязвимостях АБС и реагирование на них.

Рекомендации к проведению контроля параметров настроек технических защитных мер (выявление ошибок конфигурации) приведены в приложении 4 к настоящему документу.

10.2. Периодичность проведения работ по оценке защищенности определяется решением организации БС РФ. Для АБС, используемых для реализации банковского платежного технологического процесса, рекомендуется проведение комплексной оценки защищенности не реже одного раза в год.

10.3. Сообщения об уязвимостях программного обеспечения могут быть получены из различных источников, таких как:

— уведомления, публикуемые центрами реагирования на компьютерные инциденты (например, уведомления CERT [2]), платежными системами (например, уведомления платежной системы VISA [3]), производителями технических и программных средств (например, уведомления компании ORACLE [4]);
— уведомления, публикуемые в общедоступных базах данных уязвимостей, а также распространяемые по подписке;
— сообщения об уязвимостях в АБС, направляемые сторонними специалистами в адрес организации БС РФ или публикуемые ими в общедоступных источниках, для чего рекомендуется предусматривать способы оперативной связи с соответствующими специалистами организацией БС РФ.

10.4. Рекомендуется организовать выполнение деятельности по:

— идентификации АБС, компонентом которых является программное обеспечение с выявленными уязвимостями;
— определению степени критичности выявленных уязвимостей для реализации банковских технологических процессов организации БС РФ;
— принятию решений об устранении уязвимости в рамках мероприятий по сопровождению и модернизации АБС в случае ее подтверждения.

11. Сопровождение и модернизация АБС

11.1. Основными задачами на стадии сопровождения и модернизации АБС в части обеспечения ИБ являются:

— обеспечение проверки в тестовой среде работоспособности подсистемы ИБ АБС после обновления компонентов АБС, выполненных в рамках сопровождения АБС;
— обеспечение доработки эксплуатационной документации при изменении применяемых версий обеспечивающих компонентов АБС;
— предотвращение утечки информации в рамках работ по сопровождению АБС, в том числе с участием сторонних организаций;
— предотвращение утечки информации при передаче средств вычислительной техники на ремонт в сторонние организации;

— обеспечение контроля полноты проведения мероприятий на стадиях жизненного цикла АБС при ее модернизации.

11.2. Для предотвращения утечки информации в рамках работ по сопровождению (модернизации) АБС, в том числе с участием сторонних организаций, рекомендуется организовать контроль лиц, осуществляющих работы по сопровождению (модернизации) АБС, со стороны работников организации БС РФ с возложением ответственности за выполнение несанкционированных и (или) нерегламентированных операций, выполняемых в рамках сопровождения (модернизации), на указанных работников организации БС РФ.

11.3. Модернизация АБС включает в себя в необходимом объеме стадии разработки технического задания, проектирования, создания и тестирования, приемки и ввода в действие.

12. Стадия снятия с эксплуатации

12.1. Основными задачами на стадии снятия с эксплуатации в части обеспечения ИБ являются:

— контроль соблюдения правил и процедур обеспечения информационной безопасности при снятии с эксплуатации АБС;
— архивирование информации, содержащейся в АБС, в случае необходимости ее дальнейшего использования;
— гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации АБС и (или) уничтожение машинных носителей информации АБС в случаях, предусмотренных законодательством РФ, в том числе нормативными актами Банка России, внутренними документами организации БС РФ.

Приложение 1

Типовые недостатки в реализации функций безопасности автоматизированных систем

1. Общие недостатки АБС и банковских приложений

1.1. Управление доступом

1.1.1. Наличие у пользователя прав доступа, не являющихся безусловно необходимыми для выполнения технологических операций, предусмотренных его ролью в организации БС РФ.

1.1.2. Наличие у технологической учетной записи, от имени которой функционирует составная часть АБС, прав доступа, не являющихся безусловно необходимыми для выполнения операций, предусмотренных для этой составной части АБС проектной документацией.

1.1.3. Наличие в АБС учетных технологических записей со стандартными паролями, задаваемыми автоматически при установке программного обеспечения.

1.1.4. Реализация в АБС дискреционной, мандатной или иных моделей управления доступом вместо ролевой модели.

1.1.5. Отсутствие в АБС встроенных средств формирования отчетов о пользователях и их привилегиях.

1.1.6. Реализация функций управления доступом только на уровне АБС.

1.1.7. Наличие в графическом интерфейсе пользователя АБС элементов управления, предназначенных для выполнения операций, права на выполнение которых у пользователя отсутствуют.

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

1.2. Идентификация и аутентификация

1.2.1. Отсутствие аутентификации серверной стороны при взаимодействии пользователя с АБС и составных частей АБС между собой.

1.2.2. Взаимодействие составных частей АБС без аутентификации инициатора взаимодействия.

1.2.3. Использование протоколов аутентификации, допускающих незащищенную передачу аутентификационных данных пользователей (в том числе передачу их открытым текстом или с использованием обратимых преобразований).

1.2.4. Выполнение в алгоритмах аутентификации сужающих преобразований аутентификационных данных (например, приведение букв идентификатора пользователя и (или) пароля к одному регистру, ограничение количества значащих символов пароля).

1.2.5. Использование предсказуемых идентификаторов (например, производных от имени и фамилии пользователя, совпадающих с идентификаторами в адресах электронной почты, порядковых номеров, формирование идентификаторов по единому алгоритму).

1.2.6. Отсутствие принудительного ограничения на минимальную сложность паролей (например, ограничение минимальной длины пароля, наличие символов различных классов, несовпадение пароля с идентификатором пользователя, несовпадение нового пароля с одним из ранее использовавшихся).

1.2.7. Использование при создании новых учетных записей единого первоначального пароля или формирование таких паролей по единому алгоритму, а также отсутствие механизма принудительной смены первоначального пароля при первом входе пользователя в систему.

1.2.8. Хранение в АБС паролей пользователей с использованием обратимых преобразований. При несанкционированном доступе нарушителя к ОС или СУБД серверных компонентов АБС приводит к компрометации всех учетных записей данной АБС и отдельных учетных записей в остальных АБС организации БС РФ.

1.2.9. Использование процедур самостоятельного восстановления или смены забытых пользователями паролей.

1.2.10. Отсутствие предварительной аутентификации при смене пароля пользователем. В ряде случаев делает возможным обход аутентификации путем задания нарушителем нового пароля пользователя.

1.2.11. Отображение символов пароля при вводе.

1.2.12. Отсутствие противодействия автоматизированному подбору идентификаторов и паролей пользователей, в том числе:

— отсутствие автоматического временного блокирования учетной записи при превышении заданного количества неуспешных попыток аутентификации;
— отсутствие механизмов, исключающих возможность автоматизированного подбора паролей (например, CAPTCHA).

1.2.13. При автоматическом блокировании учетной записи в случае превышения заданного количества неуспешных попыток аутентификации — отсутствие автоматического разблокирования учетной записи по истечении заданного интервала времени, что позволяет нарушителю блокировать доступ пользователей в АБС.

1.2.14. Необходимость выполнения отдельных программных модулей АБС с правами администратора операционной системы. При наличии уязвимостей программного кода приложения позволяет нарушителю получить полный контроль над приложением и операционной системой.

1.2.15. Аутентификация пользователей средствами программного кода автоматизированного рабочего места (далее — АРМ) при отсутствии аутентификации пользователя серверными компонентами АБС, что делает возможным обход аутентификации нарушителем.

1.2.16. Наличие аутентификационных данных, необходимых для доступа компонентов АБС к прочим АБС организации БС РФ, в программном коде компонентов АБС и (или) в доступных пользователям конфигурационных файлах.

1.2.17. Использование протоколов взаимодействия, уязвимых для перехвата и повторного использования постаутентификационных данных (хеш-значений паролей, идентификаторов сессии, аутентификационных маркеров и т.п.), уязвимых к перехвату и повторному использованию.

1.3. Регистрация событий и просмотр журналов регистрации событий

1.3.1. Отсутствие или отключение средств синхронизации времени операционной системы.

1.3.2. Отсутствие механизмов регистрации отдельных типов событий, существенных для расследования инцидентов, в том числе:

— создание новых учетных записей и изменение прав доступа учетных записей;
— неуспешные операции (например, ошибки аутентификации, недостаточные права доступа при выполнении операций, недоступность интерфейсов составных частей АБС);
— срабатывание функций безопасности, направленных на противодействие компьютерным атакам (например, автоматическое блокирование учетных записей, автоматическое завершение сессий, поступление некорректных исходных данных на внешние и интерфейсы АБС);
— выполнение операций, предусмотренных моделью угроз в качестве составной части реализации угрозы.

1.3.3. Отсутствие в данных журналов регистрации событий существенных сведений о регистрируемых событиях, позволяющих установить обстоятельства наступления события.

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

1.3.5. Регистрация отдельных событий только составными частями АБС, потенциально доступными нарушителю (например, АРМ пользователя, общедоступные веб-серверы).

1.3.6. Хранение журналов регистрации событий в незащищенном виде (например, в общедоступном пользователям для изменения файле или таблице базы данных).

1.3.7. Возможность изменения пользователями параметров регистрации событий.

1.3.8. Отсутствие встроенных или специализированных средств анализа журналов регистрации событий, в том числе поиска событий по заданным критериям (по имени и идентификатору пользователя, дате, времени и т.д.).

1.3.9. Отсутствие механизмов оперативного уведомления администраторов АБС о событиях, имеющих признаки инцидента безопасности.

1.4. Обработка ввода и вывода

1.4.1. Отсутствие предварительной проверки корректности входных данных (например, проверки ограничений на длину текстовых строк, отсутствия в них недопустимых символов и комбинаций символов, соответствия числовых значений граничным условиям).

1.4.2. Наличие в видимых пользователями сообщениях об ошибках чувствительной информации (например, аутентификационных данных, сведений, идентифицирующих программное обеспечение составных частей АБС, диагностической информации).

1.4.3. Отсутствие проверки корректности выходных данных, в том числе:

— возможность формирования серверными компонентами АБС исполняемых файлов и сценариев на основе задаваемых пользователями исходных данных;
— возможность включения в выходные данные, передаваемые между составными частями АБС, фрагментов, не соответствующих спецификациям протоколов взаимодействия и (или) используемых для эксплуатации типовых уязвимостей.

1.5. Криптографическая защита

1.5.1. Использование для взаимодействия составных частей АБС (в том числе размещенных в пределах контролируемой зоны) протоколов, не обеспечивающих криптографическую защиту данных.

1.5.2. Отсутствие технологической возможности использования приложением сертифицированных СКЗИ при выполнении операций, требующих криптографической защиты данных (в том числе и в случаях, когда возможность использования несертифицированных СКЗИ предусмотрена решением руководства организации БС РФ).

1.5.3. При использовании приложением сертифицированных СКЗИ — выполнение криптографических операций с использованием программного интерфейса, характерного только для определенной модели СКЗИ.

1.5.4. Использование процедур генерации криптографических ключей, допускающих возможность копирования симметричного ключа и (или) закрытой части асимметричного ключа пользователем.

1.5.5. Использование для генерации псевдослучайных последовательностей (например, для формирования идентификаторов сессий, challenge-запросов, GUID) программных генераторов, не входящих в состав СКЗИ.

1.5.6. Использование СКЗИ в режимах и условиях, не предусмотренных эксплуатационной документацией СКЗИ.

1.6. Безопасная архитектура и разработка

1.6.1. Отказ от использования в программном коде компонентов АБС механизмов защиты, предоставляемых архитектурой процессора, операционной системой и средствами компиляции кода (например, защиты от переполнения буфера, защиты от нарушения обработки исключений, защиты от исполнения кода в сегментах стека и данных, случайного размещения сегментов в адресном пространстве).

1.6.2. Использование функций стандартных библиотек, уязвимых к атакам переполнения буфера, при наличии аналогичных функций с встроенной защитой.

1.6.3. Отсутствие предварительной инициализации переменных и структур данных при выделении оперативной памяти.

1.6.4. Присутствие в операционной системе, СУБД, серверных компонентах прикладного ПО функционирующих и доступных для взаимодействия сетевых служб, использование которых не предусматривается проектной документацией.

1.7. Защита данных

1.7.1. Отсутствие в АБС механизмов очистки остаточной информации при удалении данных.

1.7.2. Отсутствие защиты от несанкционированного доступа к разделяемым ресурсам операционной системы (например, к разделяемой памяти, именованным каналам, отображаемым в памяти файлам).

1.7.3. Некорректное использование средств синхронизации доступа к разделяемым ресурсам операционной системы (например, критических секций, семафоров).

1.8. Конфигурация безопасности

1.8.1. Отсутствие механизмов защиты от несанкционированного доступа к настройкам приложения.

1.8.2. Отсутствие возможности экспорта настроек приложения в формат, пригодный для анализа специалистом.

1.9. Контроль целостности и достоверности

1.9.1. Отсутствие в АБС средств контроля целостности программного кода и корректности настроек составных частей АБС.

1.9.2. Отсутствие механизмов обработки ошибок и отката к предыдущему состоянию при выполнении отдельных операций.

1.9.3. Отсутствие механизмов перевода АБС в аварийный режим функционирования при выявлении нарушения целостности программного кода или некорректности настроек.

1.9.4. Отключение отдельных функций безопасности при переводе АБС в аварийный режим функционирования.

1.9.5. Отсутствие механизмов генерации диагностической информации при переводе АБС в аварийный режим функционирования.

2. Типовые недостатки приложений дистанционного банковского обслуживания и электронных средств платежа

2.1. Идентификация и аутентификация

2.1.1. Использование однофакторной аутентификации при выполнении финансовых операций.

2.1.2. Предсказуемый алгоритм формирования однократных паролей и (или) возможность повторного использования однократных паролей.

2.2. Безопасность транзакций

2.2.1. Использование для подтверждения транзакций средств авторизации (например, простой электронной подписи), допускающих возможность формирования подтверждения третьими лицами, в том числе сотрудниками организации БС РФ.

2.2.2. Выбор механизмов авторизации следует осуществлять исходя из критичности транзакций и возможных проблем, которые могут быть связаны с обеспечением аутентичности и целостности данных. Примерами недостатков в реализации механизмов авторизации могут являться:

- отсутствие средств подтверждения для неплатежных операций, влияющих на платежный процесс (создание шаблонов платежных поручений, ведение справочников реквизитов получателей платежей, изменение лимитов и т.п.);
- 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;
- отсутствие сквозного контроля электронных подписей в электронном платежном документе на всех этапах его обработки.

3. Типовые недостатки веб-приложений

3.1. Размещение компонентов веб-приложения

3.1.1. Размещение в единой демилитаризованной зоне веб-серверов и иных составных частей нескольких АБС.

3.1.2. Хранение данных, используемых веб-сервером, а также журналов регистрации событий на системном разделе жесткого диска.

3.1.3. Совместное расположение журналов регистрации событий и системных файлов.

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

3.2. Управление сессиями

3.2.1. Использование предсказуемых идентификаторов сессий.

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

3.2.3. Возможность использования идентификатора сессии после ее завершения.

3.2.4. Раскрытие идентификаторов сессий, в том числе передача идентификаторов в незашифрованном виде, а также включение идентификаторов в записи журналов регистрации событий, в сообщения об ошибках.

3.3. Управление доступом

3.3.1. Отсутствие контроля доступа на уровне идентификаторов ресурсов (URI), в том числе возможность несанкционированного доступа к отдельным разделам и объектам веб-сайта путем указания их URI в веб-браузере пользователя.

3.3.2. Возможность просмотра содержимого каталогов веб-сайта в случаях, когда такой просмотр не является необходимым.

3.3.3. Использование при обработке данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype).

3.4. Защита данных

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

3.4.2. Передача конфиденциальной и аутентификационной информации в сообщениях HTTP-GET.

3.4.3. Отсутствие атрибута HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым веб-браузером.

3.4.4. Отсутствие атрибута secure у параметров cookie, содержащих чувствительную информацию.

3.5. Обработка ввода и вывода

3.5.1. Отсутствие проверки корректности вводимых пользователем данных или выполнение такой проверки только сценариями, исполняемыми веб-браузером.

3.5.2. Отсутствие директивы, определяющей используемую кодировку в заголовках сообщений HTTP, а также использование разных кодировок для разных источников входных данных.

3.5.3. Отказ от использования встроенных средств проверки корректности входных параметров, реализованных в стандартных программных библиотеках.

3.5.4. Отсутствие или отключение средств предотвращения атак, связанных с использованием типовых уязвимостей веб-приложений.

3.5.5. Отсутствие средств контроля корректности входных данных, предназначенных для последующей обработки программными модулями, допускающими интерпретацию команд (SQL, XPath, LINQ, LDAP, командная оболочка ОС и т.п.).

3.5.6. Отсутствие преобразования специальных символов, предусмотренного спецификациями языка HTML (например, замены символов ‘<’ и ‘>’ специальными символами языка HTML).

4. Типовые недостатки систем управления базами данных

4.1. Функционирование и доступность протоколов взаимодействия с СУБД, использование которых не предусмотрено проектной документацией.

4.2. Возможность доступа составных частей АБС к функциям СУБД без аутентификации.

4.3. Наличие у администраторов СУБД учетных записей операционной системы с правами, не являющимися безусловно необходимыми для обслуживания СУБД.

4.4. Наличие у технологических учетных записей, используемых составными частями АБС для доступа к СУБД, прав, не являющихся безусловно необходимыми для выполнения предусмотренных документацией операций.

4.5. Установка СУБД на сервер, используемый другими составными частями АБС.

4.6. Размещение СУБД в демилитаризованной зоне, в которую возможен непосредственный доступ внешних пользователей.

4.7. Возможность доступа к системным таблицам и конфигурационным настройкам у пользователей, не являющихся администраторами.

4.8. Наличие в СУБД демонстрационных баз данных, поставляемых в составе дистрибутива программного обеспечения СУБД.

4.9. Размещение данных нескольких приложений в одном разделе СУБД в случае, когда такое размещение не предусмотрено явно проектной документацией.

5. Типовые недостатки операционных систем

5.1. Управление доступом

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

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

5.1.3. Возможность доступа к настройке параметров операционной системы, заданий, журналу событий, системным файлам у пользователей, не являющихся администраторами ОС.

5.1.4. Задание индивидуальных прав доступа к объектам операционной системы отдельным пользователям (вместо включения этих пользователей в соответствующие группы).

5.1.5. Возможность интерактивного входа в систему для системных учетных записей, использующихся приложениями и сервисами.

5.1.6. Наличие у пользователя, не являющегося администратором ОС, прав на чтение и (или) модификацию файлов в домашних каталогах остальных пользователей.

5.1.7. Отсутствие дисковых квот для учетных записей (включая технологические учетные записи).

5.1.8. Несоответствие настроек операционной системы рекомендациям разработчика по ее безопасной настройке.

5.1.9. Наличие в операционных системах серверных компонентов АБС программного обеспечения, не предусмотренного эксплуатационной документацией.

5.2. Идентификация и аутентификация

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

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

5.2.3. Отсутствие аутентификации пользователя при доступе к параметрам BIOS, параметрам загрузчика ядра ОС, входе в режим восстановления системы (safe mode, single-user mode и т.п.).

5.3. Управление системой

5.3.1. Отключение в настройках ядра операционной системы механизмов, настройки ядра, предотвращающих выполнение кода в области данных и стека.

5.3.2. 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.

5.3.4. Включенная в настройках операционной системы возможность гибернации (перехода в ждущий режим).

5.3.5. Отключение встроенного межсетевого экрана операционной системы, отсутствие в настройках встроенного межсетевого экрана правил фильтрации, блокирующих взаимодействие, не предусмотренное эксплуатационной документацией АБС, и отключение используемых средств защиты сторонних производителей.

6. Типовые недостатки телекоммуникационного оборудования

6.1. При возможности выбора операционной системы для установки на телекоммуникационное оборудование — установка операционных систем с заведомо избыточными функциональными возможностями.

6.2. Использование в телекоммуникационной инфраструктуре АБС коммутационного оборудования, не обеспечивающего возможность отключения неиспользуемых интерфейсов и контроль подключения сетевых устройств (например, по MAC-адресам или с использованием протокола IEEE 802.1x), защиту от атак типа ARP spoofing, разделение сети на сегменты с использованием технологии VLAN.

6.3. Настройка сегментов VLAN, допускающая присутствие в одном сегменте АРМ пользователей и серверов АБС, а также АРМ пользователей и АРМ администраторов АБС.

7. Типовые недостатки технологий виртуализации

7.1. Возможность доступа к данным виртуальных машин (например, настройкам виртуального аппаратного обеспечения, образам дисков) пользователей, не являющихся администраторами сервера виртуализации.

7.2. Предоставление виртуальным машинам доступа к разделяемым ресурсам операционной системы сервера виртуализации в случаях, когда такой доступ не предусмотрен явно эксплуатационной документацией АБС.

7.3. Отсутствие средств мониторинга объема свободных ресурсов сервера виртуализации.

7.4. Отсутствие ограничения удаленного доступа администраторов сервера виртуализации путем ограничения IP-адресов, с которых разрешен доступ, и сетевого интерфейса для доступа администраторов.

7.5. Использование для удаленного администрирования сервера виртуализации сетевых интерфейсов, используемых виртуальными машинами.

7.6. Хранение журналов регистрации событий средств виртуализации в каталогах, доступных на чтение и (или) запись виртуальным машинам.

7.7. Использование в виртуальных машинах образов жестких дисков с динамически изменяемым размером.

7.8. Непосредственный доступ виртуальных машин к физическим дискам и логическим томам памяти сервера виртуализации.

7.9. Использование в графическом интерфейсе сервера виртуализации расширенных механизмов обмена данными между виртуальными машинами и сервером виртуализации (например, drag and drop, copy and paste).

7.10. Использование расширенных механизмов обмена данными между виртуальными машинами (например, программного интерфейса сервера виртуализации, виртуальных сокетов).

7.11. Возможность изменения пользователем режима загрузки виртуальной машины.

Приложение 2

Рекомендации к проведению контроля исходного кода

1. Общие положения

1.1. Контроль кода (code review) — мероприятия, осуществляемые в отношении определенных частей исходного текста (исходного кода) программы для ЭВМ, созданных одним или несколькими разработчиками, другим (не создававшим эту часть кодов) разработчиком или назначенным в установленном порядке иным имеющим требуемую подготовку специалистом, и которые состоят в детальной проверке (изучении, анализе, исследовании) соответствующих исходных кодов с целью выявления неизвестных уязвимостей, в том числе связанных с ошибками программирования, нарушений установленных требований, а также иных существенных дефектов.

1.2. Объектом исследования являются тексты программ разрабатываемых компонентов АБС, в первую очередь тексты программ специализированных банковских приложений.

1.3. Контроль кода может в обоснованных случаях проводиться несколькими лицами, в том числе при участии создавшего и (или) модифицировавшего проверяемый код разработчика.

1.4. Контроль кода может осуществляться лицом, проверяющим код, как вручную, в том числе с использованием приемов эффективного чтения программного кода (code reading), так и с применением методов и средств автоматизированного анализа исходного кода, в том числе обеспечивающих:

— статический анализ кода;
— динамический анализ кода.

2. Контроль кода вручную

2.1. Контроль (проверка) исходного кода вручную обеспечивается просмотром, изучением и оценкой кода лицом, отличным от его разработчика. Оценка кода может включать в себя:

— оценку соответствия кода требованиям, предъявляемым к структурированию и оформлению кода, именованию объектов, разделению на модули, использованию специальных средств обеспечения качества кода, предусмотренных используемыми языками программирования и средствами разработки;
— оценку полноты и качества документирования кода, включая документирование заголовков программных модулей, прототипов функций и структур данных, комментарии к выполнению существенных операций;
— оценку соответствия алгоритмов, реализованных в исходном коде, программной документации, в том числе выявление явных недекларированных возможностей (программных закладок), ошибок программного кода, попыток запутывания (обфускации) программного кода и использования иных приемов, затрудняющих проведение контроля.

2.2. Методы эффективного чтения кода включают двойное чтение (сначала понять общую структуру, запомнить основные обозначения и соглашения, затем читать снова, выявляя дефекты, несоответствия), использование сценариев и др.

2.3. Помимо приемов индивидуальной проверки кода, существуют методы эффективной организации взаимодействия участников контроля кода, в том числе прослеживания (walkthrough), инспекции кода (code inspections) и др. Они являются достаточно ресурсоемкими и для их применения нужны соответствующие навыки, но при рациональном использовании они могут быть весьма эффективны в случаях, требующих особого внимания.

3. Статический анализ кода

3.1. Статический анализ кода (static_program_analysis) проводится с использованием автоматизированных средств (программных инструментов) и направлен на идентификацию потенциально опасных фрагментов кода, в том числе:

— вызовов функций, методов, процедур (далее — функции) с передачей им в качестве аргументов данных, вводимых пользователем или принимаемых из внешних источников;
— текстов функций преобразования форматов данных;
— вызовов системных функций и функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС, в том числе функций обеспечения ИБ операционной системы и специализированных технических защитных мер, функций ввода/вывода, управления памятью и системными ресурсами;

— текстов функций, осуществляющих проверку прав доступа и принятие решений, основанных на значениях атрибутов безопасности;
— текстов функций, самостоятельно реализующих функциональность обеспечения ИБ, в том числе криптографические функции, аутентификацию пользователей и проверку прав доступа, генерацию данных мониторинга ИБ;
— текстов функций, предусматривающих установление соединения с внешними компонентами с передачей им аутентификационных данных;
— текстов обработчиков ошибок и исключений.

3.2. В ходе статического анализа кода рекомендуется проводить поиск типовых ошибок программирования (недостаточная проверка входных параметров функций, включение аутентификационных данных непосредственно в текст программ, некорректное преобразование типов, недостаточная обработка ошибок и исключений), а также определяются статические пути исполнения программы.

4. Динамический анализ кода

4.1. Динамический анализ кода осуществляется путем выполнения или эмуляции выполнения программы на определенной совокупности наборов тестовых исходных данных. Перед выполнением или в процессе выполнения программа иногда инструментируется путем дополнения ее функциями трассировки выполнения для задания и контроля инвариантов, предусловий, постусловий и др. Динамический контроль проводится с использованием специализированных автоматизированных средств и может включать в себя, в частности:
— исследование особенностей исполнения потенциально опасных функций при задании заведомо некорректных аргументов;
— построение динамических путей исполнения программы и идентификацию точек принятия решений, существенных для выполнения функций обеспечения ИБ;
— поиск чувствительной информации в оперативной памяти и в аргументах функций;
— исследование особенностей исполнения программы при типовых атаках (переполнение буфера, внедрение операторов SQL в данные, используемые для формирования запросов к СУБД).

5. Дополнительные практические аспекты контроля кода

5.1. Вне зависимости от применяемых способов и методов анализа кода при его осуществлении рекомендуется использование классификаторов типовых ошибок программирования, а также способов выявления различных типов ошибок, например каталог Common Weakness Enumeration [5].

5.2. Выявленным в рамках контроля кода уязвимостям в коде разрабатываемых компонентов АБС целесообразно присваивать оценку степени их критичности (например, высокая, средняя, низкая) для обеспечения ИБ организации БС РФ. Для каждой выявленной уязвимости с учетом ее критичности принимается решение о доработке программного компонента АБС (и о приоритетности доработки) или о принятии рисков, связанных с наличием уязвимости.

5.3. Результаты контроля кодов оформляются протоколами контроля кода (название этих документов может быть иным), подписываемыми разработчиками — непосредственными исполнителями разработки проверенного исходного кода и лицами, участвовавшими в его проверке (контролерами кода), с отражением в протоколе сведений о дате мероприятия, проверенной части исходных кодов, выявленных уязвимостях и иных дефектах (при наличии), повторном контроле кодов с подтверждением устранения выявленных уязвимостей, дефектов.

Примечание. Протоколы контроля кода и иные подобные документы целесообразно оформлять в виде информации в электронной форме, созданной, переданной и надежно сохраненной в предусмотренной для данного вида информации (документов) системе электронного документооборота (например, в архиве сообщений электронной почты), с реквизитами (название, уникальный номер, подписи, даты и др.), позволяющими при аудите предъявлять ее в качестве электронного документа (комплекта документов), подписанного простыми электронными подписями, а также при необходимости изготавливать и заверять ее копии на бумажном носителе. (Требование об оформлении протоколов изначально на бумажном носителе или с усиленными электронными подписями может блокировать систематическое выполнение контроля кода.)

5.4. Мероприятия по контролю кода планируются и осуществляются в отношении всего подлежащего контролю измененного или вновь созданного исходного кода с уведомлением и в необходимых случаях при участии представителей службы ИБ в качестве контролеров кода.

Приложение 3

Рекомендации к проведению оценки защищенности

Оценка защищенности заключается в исследовании АБС или ее компонентов, целью которого является выявление уязвимостей, которые могут быть использованы злоумышленником для реализации угроз ИБ. Выделяются следующие основные методы оценки защищенности:

— тестирование на проникновение;
— выявление известных уязвимостей программного обеспечения.

1. Тестирование на проникновение

1.1. Описание метода

1.1.1. Тестирование на проникновение является основным методом оценки защищенности, охватывающим все аспекты функционирования подсистемы ИБ АБС, включая действия персонала по реагированию на инциденты ИБ и противодействие компьютерным атакам.

1.1.2. Достоинствами тестирования на проникновение как метода оценки защищенности являются:

— высокая достоверность сведений о выявленных уязвимостях за счет фактического подтверждения возможности их использования злоумышленником;
— достаточность результатов исследования для оценки критичности выявленных уязвимостей;
— наглядность получаемых результатов.

Недостатками тестирования на проникновение являются:

— способность исследователя воспроизводить только действия нарушителя, равного или уступающего по квалификации, как следствие — высокие требования к квалификации исследователя и низкая достоверность сведений об отсутствии уязвимостей;
— низкая степень автоматизации действий исследователя, как следствие — высокие трудозатраты по сравнению с другими способами оценки защищенности.

1.1.3. При тестировании на проникновение исследователь выполняет поиск уязвимостей АБС, воспроизводя действия злоумышленника. Перед началом работ для исследователя создаются условия, эквивалентные тем, в которых действует потенциальный злоумышленник. Условия проведения тестирования на проникновение различаются по следующим показателям:

— наличие прав доступа у исследователя в АБС;
— расположение исследователя относительно сетевого периметра защиты АБС;
— стратегия предоставления исследователю информации об АБС.

1.1.4. Тестирование на проникновения подразделяется на исследования с предоставлением доступа к АБС и без предоставления такого доступа. При исследовании с предоставлением доступа исследователю предоставляются учетные записи для доступа к АБС. При исследовании без предоставления доступа к АБС задача самостоятельного получения учетных записей пользователей АБС является составной частью тестирования на проникновение.

1.1.5. По расположению исследователя относительно сетевого периметра АБС тестирование на проникновение разделяется на внешнее и внутреннее. При внутреннем тестировании на проникновение исследователю предоставляется возможность подключения к телекоммуникационному оборудованию в точке, находящейся внутри сетевого периметра защиты организации БС РФ и обеспечивающей возможность сетевого взаимодействия с составными частями АБС. При внешнем тестировании на проникновение начальные действия исследователя ограничены только сетевыми протоколами взаимодействия с АБС, доступными извне сетевого периметра защиты организации БС РФ. При отсутствии в АБС интерфейсов для взаимодействия извне сетевого периметра задача самостоятельного преодоления сетевого периметра защиты организации БС РФ является составной частью тестирования на проникновение.

1.1.6. При тестировании на проникновение могут использоваться две стратегии предоставления исследователю информации об АБС. При стратегии черного ящика исследователь оперирует только теми сведениями об АБС, которые получены им самостоятельно в ходе тестирования на проникновение. При стратегии белого ящика исследователю заблаговременно предоставляется вся доступная информация об АБС, включая при наличии проектную и эксплуатационную документацию, исходные коды программных компонентов АБС и возможность просмотра параметров настройки компонентов АБС.

1.1.7. Рекомендуется проведение тестирования на проникновение только с уведомлением эксплуатирующего персонала организации БС РФ с исключением возможности активного противодействия исследователю.

1.1.8. Перед проведением тестирования на проникновение рекомендуется определить начальные условия его проведения. Рекомендуется учитывать, что максимальная полнота оценки достигается при внутреннем тестировании на проникновение с использованием предоставленного доступа к АБС и стратегией белого ящика. Тестирование на проникновение при таких начальных условиях рекомендуется проводить на стадии приемки и ввода в эксплуатацию, а также после каждой модернизации АБС.

1.1.9. Любые действия, выполнение которых способно причинить ущерб организации БС РФ, выполняются только после их подтверждения руководством организации БС РФ.

1.1.10. В ходе тестирования на проникновение возможно получение исследователем доступа к сведениям, охраняемым в соответствии с законодательством РФ и нормативными документами организации БС РФ. Трудовые договоры с работниками организации БС РФ, договоры оказания услуг с организациями, проводящими тестирование на проникновение, должны включать в себя:

— требование о сохранении конфиденциальности сведений, доступ к которым потенциально может быть получен в ходе тестирования на проникновение, в соответствии с законодательством РФ, в том числе нормативными актами Банка России и документами организации БС РФ;
— распределение и установление ответственности для случаев, когда выполнение действий в рамках тестирования на проникновение приведет к негативным последствиям и ущербу для организации БС РФ.

1.1.11. Отчет о тестировании на проникновение должен содержать:

— описание начальных условий исследования и постановку задачи;
— описание последовательности действий, которые приводили к выявлению уязвимостей или изменению возможностей исследователя, а также решения об отказе от выполнения запрашиваемых действий;
— описание выявленных уязвимостей, оценку степени их критичности для обеспечения ИБ организации БС РФ;
— рекомендации по устранению выявленных уязвимостей.

1.2. Содержание работ по тестированию на проникновение

1.2.1. Тестирование на проникновение включает в себя следующие направления исследований:

— оценка защищенности сетевого периметра, сетевых устройств и протоколов;
— оценка защищенности беспроводных сетей;
— оценка защищенности веб-приложений;
— оценка защищенности операционных систем;
— оценка защищенности систем управления базами данных (СУБД);
— оценка защищенности средств виртуализации;
— оценка защищенности специализированных банковских приложений;
— оценка защищенности мобильных устройств.

1.2.2. При проведении оценки защищенности сетевого периметра, сетевых устройств и протоколов рекомендуются следующие мероприятия:

— идентификация доступных исследователю сетевых устройств и протоколов взаимодействия;
— идентификация типов устройств, а также семейств и версий программного обеспечения, реализующего сетевые протоколы, на основе предоставляемой ими информации и особенностей их реакции на взаимодействие;
— поиск интерфейсов удаленного доступа и прочих интерфейсов взаимодействия, доступность которых из данной точки не предусмотрена требованиями ИБ организации БС РФ или практикой создания защищенных автоматизированных систем;
— проверка возможностей перенаправления сетевого трафика с использованием особенностей протоколов канального и сетевого уровня, протоколов автоматического взаимного согласования параметров телекоммуникационного оборудования, создания ложных сетевых служб автоматической адресации, разрешения имен, создания ложных сетевых служб;
— подбор данных аутентификации (имен пользователей, паролей, ключей) для доступа к сетевым службам на основе словарей стандартных и часто встречающихся значений;

— перехват и повторная отправка данных аутентификации;
— проверка возможности обхода средств защиты сетевого периметра путем изменения значимых полей сетевых пакетов, туннелирования и шифрования данных, перегрузки журналов событий СЗИ незначащей информацией;
— идентификация доступных веб-интерфейсов и нестандартных протоколов взаимодействия для последующего анализа.

1.2.3. При проведении оценки защищенности беспроводных сетей рекомендуются следующие мероприятия:

— прослушивание трафика, в том числе обнаружение доступных беспроводных сетевых устройств и их идентификаторов, определение текущей зоны радиовидимости, сбор информации о клиентских устройствах (например, MAC-адреса), сбор доступных идентификаторов сетей, определение применяемых алгоритмов шифрования;
— рассылка пробных запросов (например, для перебора идентификационных данных устройств) и анализ ответов на пробные запросы;
— выявление недостатков в настройке встроенных средств криптографической защиты беспроводных устройств;
— навязывание клиентским устройствам ложных точек доступа или дубликатов точек доступа.

1.2.4. При проведении оценки защищенности веб-приложений рекомендуются следующие мероприятия:

— выявление уязвимостей, связанных с раскрытием чувствительной информации о приложении, в том числе путем отправки некорректных сообщений, анализа стандартных системных сообщений об ошибках, поиска чувствительной информации в коде и комментариях веб-страниц;
— получение сведений о структуре файловой системы перебором путей и имен файлов (полный перебор, перебор по словарю, проверка наличия стандартных файлов используемых платформ и средств разработки, поиск резервных копий файлов);
— проверка корректности обработки специальных символов в параметрах запроса (символы форматирования вывода, перевода строки и возврата каретки, перехода в вышестоящий каталог, двойное URL-кодирование);
— проверка корректности обработки параметров различной длины;
— проверка корректности обработки числовых параметров, в том числе не предусмотренных технологией обработки больших величин, отрицательных и нулевых значений;
— проверка корректности приведения и преобразования типов параметров;
— проверка корректности обработки различного представления пользовательских данных, в том числе дублирование заголовков запроса, дублирование параметров сценария;
— проверка корректности обработки параметров универсального идентификатора ресурса (URI — uniform resource identifier), в том числе возможности подключения произвольного внешнего источника данных, или перенаправления на внешний или внутренний веб-сайт, возможности обращения к сетевым протоколам, возможности замены полного пути к ресурсу на относительный;
— проверка наличия ошибок, связанных с обработкой загружаемых файлов, в том числе с обработкой имен файлов без расширения, несоответствием расширения типу файла, альтернативными расширениями для файлов одного типа, специальными символами (включая нулевой символ) в имени файла;
— проверка корректности исполнения сценариев при манипулировании входными параметрами, в том числе атрибутами безопасности, используемыми при управлении доступом;
— проверка возможности подбора аутентификационных данных (паролей, включая словарные, идентификаторов сессий, атрибутов, используемых для восстановления паролей);
— проверка корректности обработки идентификаторов сессий пользователей, в том числе обработки событий завершения сессии, интервалов неактивности, сопоставление идентификатора сессии с дополнительными атрибутами, прямо или косвенно идентифицирующими пользователя или его рабочее место, предотвращение повторного и множественного использования идентификаторов сессий;
— проверка корректности реализации механизмов авторизации;
— проверка корректности противодействия атакам на клиентские приложения, в том числе с использованием межсайтового выполнения сценариев и подделки межсайтовых запросов;

— проверка корректности обработки входных параметров сценариев при внедрении в них команд операционных систем, синтаксических конструкций языков программирования и разметки;
— проверка невозможности обхода средств межсетевого экранирования прикладного уровня путем фрагментации данных, смешивания параметров, замены алгоритма кодирования и формата представления данных, замены специальных символов их альтернативными представлениями.

1.2.5. При проведении оценки защищенности операционных систем рекомендуются следующие мероприятия:

— идентификация сетевых служб операционной системы по типовым атрибутам (стандартные параметры сетевых протоколов, характерный отклик на установление соединения, характерные особенности реализации сетевых протоколов), наличия характерных служебных сообщений в сетевом трафике;
— проверка корректности ограничения доступа к сетевым службам операционной системы, в том числе с использованием анонимного/гостевого доступа, подбора паролей, перехвата и повторного/множественного использования авторизационных маркеров;
— проверка корректности противодействия подбору паролей, в том числе оценка возможности злоумышленника блокировать учетные записи пользователей множественными неуспешными попытками аутентификации;
— проверка возможности получения злоумышленником чувствительной информации с помощью служебных сетевых протоколов (SNMP, RPC, CIFS);
— проверка возможности реализации компьютерных атак с использованием уязвимостей сетевых служб, а для автоматизированных рабочих мест — и прикладного программного обеспечения.

При наличии у исследователя доступа к интерфейсам управления операционной системой оценка защищенности дополнительно включает в себя:

— возможность загрузки операционной системы в специальном режиме или с отчуждаемого носителя (при физическом доступе к средству вычислительной техники), а также загрузку операционной системы в специальном режиме (например, в режиме восстановления);
— получение имен пользователей;
— просмотр данных журналов регистрации событий и остаточной информации (удаленных файлов, образов оперативной памяти, сохраняемых при сбоях);
— поиск аутентификационных данных пользователей в остаточной информации, конфигурационных параметрах программного обеспечения, исходном коде приложений и скриптов;
— проверку возможности передачи управления операционной системой удаленному компьютеру с установлением реверсивного соединения и туннелированием сетевых протоколов;
— проверку возможности повышения привилегий с использованием локально эксплуатируемых уязвимостей и ошибок в настройке программного обеспечения;
— перенаправление и прослушивание сетевого трафика в доменах коллизий анализируемого средства вычислительной техники путем подделки таблиц протокола ARP, подложных серверов динамической конфигурации оборудования и разрешения имен.

1.2.6. При проведении оценки защищенности СУБД рекомендуются следующие мероприятия:

— проверка корректности функционирования механизмов идентификации, аутентификации и управления доступом при взаимодействии с интерфейсами управления СУБД, в том числе блокирования анонимного и гостевого доступа, отсутствие стандартных учетных записей и учетных записей со словарными паролями;
— проверка корректности обработки модифицированных входящих запросов, включая замену параметров протокола, вставку специальных символов и команд операционной системы в параметры входящих запросов языка SQL;
— эксплуатация уязвимостей в сетевых службах СУБД.

При наличии доступа к интерфейсам управления операционной системы и СУБД дополнительно проводятся:

— проверка корректности прав доступа к файлам СУБД;
— проверка контроля целостности исполняемых файлов СУБД, включая защиту от подмены файлов;
— поиск чувствительной информации (в том числе паролей пользователей) в служебных файлах (файлы баз данных, журналов, резервных копий, конфигурации, истории команд), а также переменных системных процессов СУБД;

— эксплуатация уязвимостей в хранимых процедурах, направленная на повышение привилегий, выполнение произвольных команд или прямой доступ к содержимому таблиц, изменение системных настроек;
— проверка возможности использования хранимых процедур для доступа к защищаемым объектам СУБД и операционной системы;
— проверка корректности обработки нестандартных значений параметров хранимых процедур (передача произвольных значений параметров, внедрение операторов SQL и команд PL/SQL, T-SQL, использование курсоров; передача значений параметров различной длины);
— проверка возможности чтения чувствительной информации приложений, включая восстановление паролей пользователей СУБД и приложений из хеш-значений.

1.2.7. При проведении оценки защищенности средств виртуализации рекомендуются мероприятия по проверке возможности доступа к интерфейсам управления средой виртуализации и защищаемым объектам, в том числе:
— проверка возможности подбора паролей к интерфейсам управления;
— проверка корректности прав доступа пользователей к объектам виртуализации, включая проверку возможности несанкционированного чтения и изменения виртуальных дисков, образов оперативной памяти, конфигурационных файлов и снимков виртуальных машин;
— использование уязвимостей гипервизора и средств управления средой виртуализации.

1.2.8. При проведении оценки защищенности специализированных банковских приложений рекомендуются следующие мероприятия:
— прослушивание сетевого трафика и поиск в нем чувствительной информации, включая пароли и хеш-значения паролей пользователей, идентификаторы сессий, авторизационные маркеры, криптографические ключи;
— запуск программ с различными параметрами, в том числе нестандартными, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования;
— мониторинг характера взаимодействия приложения с операционной системой в процессе функционирования, включая идентификацию файлов данных, содержащих чувствительную информацию, трассировку системных вызовов;
— проверка прав доступа к файлам данных, содержащим чувствительную информацию, а также контроль целостности исполняемых файлов приложения.

1.2.9. При проведении оценки защищенности мобильных устройств рекомендуются следующие мероприятия:
— проверка наличия чувствительной информации в файлах данных, журналах регистрации событий, в оперативной памяти устройства, а также передачи чувствительной информации в незашифрованном виде;
— проверка возможности чтения ключей шифрования и электронной подписи, а также записи и замены сертификатов ключей;
— идентификация протоколов взаимодействия и проверка возможности принудительного навязывания устройству использования незащищенных версий протоколов (HTTP вместо HTTPS, TELNET вместо SSH, SSH1 вместо SSH2);
— проверка корректности обработки мобильным приложением входящих параметров, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования.

2. Выявление известных уязвимостей

2.1. Выявление известных уязвимостей включает в себя:
— выявление известных уязвимостей в сетевых службах;
— выявление типовых уязвимостей в веб-приложениях;
— выявление известных уязвимостей в программном обеспечении;
— выявление учетных записей с паролями, содержащимися в словарях, используемых при проведении исследования.

Данный метод оценки защищенности может являться составной частью метода тестирования на проникновение, не требует наличия у исследователя специальных навыков и допускает полную автоматизацию.

2.2. Известные уязвимости могут быть выявлены следующими способами:

— идентификацией наименований и версий программного обеспечения АБС и поиском в базах данных известных для них уязвимостей;
— запуском тест-программ (эксплойтов), воспроизводящих в полном объеме или частично выполнение компьютерных атак с использованием известных уязвимостей.

2.3. В зависимости от начальных условий для выявления известных уязвимостей могут использоваться стратегии черного ящика и белого ящика.

При стратегии черного ящика исследователю предоставляется доступ к составным частям АБС на уровне протокола IP. Предметом исследования являются уязвимости сетевых служб компонентов АБС, доступных исследователю.

При стратегии белого ящика исследователю предоставляется доступ к интерфейсам управления операционными системами, телекоммуникационным оборудованием, СУБД и серверами приложений с необходимыми правами доступа. Предметом исследования являются все уязвимости программных компонентов АБС, сведения о которых содержатся в используемой исследователем базе данных уязвимостей.

При стратегии белого ящика исследования могут проводиться как с использованием автоматизированных средств анализа защищенности, так и вручную, при стратегии черного ящика исследования проводятся с использованием автоматизированных средств.

2.4. К достоинствам выявления известных уязвимостей как метода оценки защищенности относятся:

— высокая достоверность сведений о выявленных уязвимостях при использовании стратегии белого ящика;
— высокая степень автоматизации, низкие требования к квалификации исследователя при использовании автоматизированных средств анализа защищенности;
— пригодность результатов исследования для оценки степени возможности реализации угроз и степени тяжести последствий из реализации;
— воспроизводимость исследования.

Недостатками выявления известных уязвимостей как метода оценки защищенности являются:

— низкая достоверность сведений о выявленных уязвимостях при использовании стратегии черного ящика;
— возможность сбоев и отказов в функционировании компонентов АБС при проведении исследования с использованием стратегии черного ящика;
— необходимость предоставления исследователю привилегированного доступа к составным частям АБС при использовании стратегии белого ящика.

2.5. Выявление известных уязвимостей в сетевых службах производится при использовании стратегии черного ящика. Исследование включает в себя:

— идентификацию серверов и рабочих мест по их IP-адресам или именам;
— идентификацию сетевых протоколов, доступных для взаимодействия;
— идентификацию программ, обеспечивающих реализацию указанных сетевых протоколов, с определением их наименований и версий по информации, передаваемой при сетевом взаимодействии;
— выборку из базы данных уязвимостей, относящихся к идентифицированным версиям программ;
— выявление уязвимостей сетевых служб путем запуска потенциально применимых к ним эксплойтов.

2.6. Выявление типовых уязвимостей в веб-приложениях производится при использовании стратегии черного ящика. Исследование включает в себя выявление следующих типов уязвимостей:

— инъекции, в особенности SQL-инъекции, OS Command, LDAP и XPath-инъекции;
— подбор аутентификационных данных;
— небезопасная передача данных, в том числе в процессе аутентификации;
— ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход директорий);
— межсайтовый скриптинг (XSS);
— подделка межсайтовых запросов (CSRF);
— расщепление запроса HTTP, сокрытие ответа HTTP;
— открытое перенаправление;
— раскрытие информации о директориях/сценариях;
— предсказуемое расположение ресурсов;

— идентификация приложений;
— чтение произвольных файлов;
— раскрытие чувствительной информации;
— обратный путь в директориях;
— переполнение буфера.

Исследование производится путем анализа данных веб-форм, отправки веб-серверу тестовых запросов с варьируемыми значениями параметров запроса и анализа ответов.

2.7. Идентификация известных уязвимостей программного обеспечения выполняется с использованием стратегии белого ящика. Исследование включает в себя:

— инвентаризацию программного обеспечения, установленного на исследуемом техническом средстве, с идентификацией наименований и версий программ, а также установленных обновлений безопасности;
— выборку из базы данных уязвимостей, относящихся к идентифицированным версиям программ;
— исключение из полученной выборки уязвимостей, устранение которых обеспечено установленными обновлениями безопасности.

2.8. Выявление учетных записей с паролями, содержащимися в словарях, используемых при проведении исследования с использованием стратегий как черного ящика, так и белого ящика. При использовании стратегии черного ящика производятся попытки аутентификации с использованием имен и паролей из используемого словаря. При использовании стратегии белого ящика производятся выборка хеш-значений паролей из конфигурационных файлов, таблиц баз данных и сравнение их с хеш-значениями паролей из используемого словаря.

2.9. По результатам исследования разрабатывается отчет, содержащий:

— перечень компонентов АБС;
— перечень выявленных уязвимостей, оценку степени их критичности для обеспечения ИБ организации БС РФ;
— рекомендации по устранению выявленных уязвимостей.

Оценку критичности уязвимостей рекомендуется определять в соответствии с методикой Common Vulnerability Scoring System (CVSS).

Приложение 4

Рекомендации к проведению контроля параметров настроек технических защитных мер (выявление ошибок конфигурации)

1. Выявление ошибок конфигурации направлено на поддержание корректности функционирования подсистемы ИБ АБС. Для этого в составе рабочей документации АБС или в качестве отдельных внутренних документов организации БС РФ разрабатываются и утверждаются стандарты конфигурации программных и аппаратных компонентов АБС. Выявление ошибок конфигурации — исследование, направленное на поиск несоответствий между фактическими значениями параметров технических мер защиты и их эталонными значениями, установленными в стандартах конфигурации.

2. Исследователю должен быть предоставлен доступ к интерфейсам программных компонентов АБС, в том числе к операционной системе, специализированным банковским приложениям или альтернативный способ получения фактических параметров настройки технических мер защиты.

3. Исследование проводится с использованием стратегии белого ящика. Исследование может проводиться вручную или с использованием автоматизированных средств анализа защищенности. Ошибки конфигурации выявляются путем получения фактических значений параметров настроек и сравнения их с эталонными значениями. При этом:

— в случае, если фактическое значение параметра настройки задано явно, производится его сравнение с эталонным значением;
— в случае, если фактическое значение параметра конфигурации не задано или задано неявно, производится вычисление эффективного значения параметра настройки, которое затем сравнивается с эталонным значением.

Если параметр настройки не задан явно, устройство или программа использует значение по умолчанию, которое может зависеть от модели устройства или версии программы. В ряде случаев фактические параметры настройки задаются не явно, а в виде выражений, результаты вычисления которых зависят от фактических значений других параметров, переменных окружения. В этих случаях в ходе исследования должны быть определены эффективные значения параметров настройки с учетом особенностей их определения в рамках исследуемого компонента АБС.

4. Достоинствами данного метода являются:

— высокая достоверность сведений о выявленных несоответствиях стандартам конфигурации;
— высокая степень автоматизации, низкие требования к квалификации исследователя при использовании автоматизированных средств анализа;
— воспроизводимость исследования.

5. Недостатками данного метода являются:

— невозможность в ряде случаев оценить потенциал реализации каких-либо угроз при несоответствии отдельных настроек стандартам конфигурации. Одним из источников разработки стандартов конфигурации являются рекомендации разработчиков программного и аппаратного обеспечения. Как правило, разработчики не раскрывает информацию об угрозах, реализация которых становится возможной при невыполнении этих рекомендаций;
— необходимость предоставления исследователю привилегированного доступа к компонентам АБС;
— высокие требования к квалификации исследователя в случае, когда необходимо вычисление эффективных значений параметров конфигурации, а также в случае проведения исследования без использования автоматизированных средств анализа.

6. По результатам исследования разрабатывается отчет, содержащий перечень исследованных компонентов АБС, перечень выявленных несоответствий стандартам конфигурации и рекомендации по их устранению.

7. В случае если изменение параметров настройки не было вызвано технической необходимостью, рекомендуется проведение оперативной перенастройки компонентов АБС.

Если изменение параметров настройки было вызвано технической необходимостью и возврат к эталонным значениям может повлечь нарушение функционирования АБС, рекомен-

дуется проведение оценки критичности влияния значений параметров настройки на защищенность АБС. В случае отсутствия такого влияния или несущественного увеличения рисков нарушения ИБ рекомендуется внесение соответствующих изменений в эксплуатационную документацию (стандарты конфигурации). В случае существенного увеличения рисков нарушения ИБ рекомендуется проведение модернизации АБС или ее отдельных компонентов.

Библиография

1. National Checklist Program Repository [Электронный ресурс]: офиц. сайт. США. URL: http://web.nvd.nist.gov/view/ncp/repository (дата посл. обращения: 25.03.2014).
2. Уведомления CERT [Электронный ресурс]: офиц. сайт. URL: http://www.us-cert.gov/ncas/bulletins (дата посл. обращения: 25.03.2014).
3. Alerts, Bulletins & Webinars [Электронный ресурс]: офиц. сайт. США. URL: http://usa.visa.com/merchants/risk_management/cisp_alerts.html#anchor_3 (дата посл. обращения: 25.03.2014).
4. Critical Patch Updates, Security Alerts and Third Party Bulletin [Электронный ресурс]: офиц. сайт. США. URL: http://www.oracle.com/technetwork/topics/security/alerts-086861.html (дата посл. обращения: 25.03.2014).
5. CCE List — Archive [Электронный ресурс]: офиц. сайт. США. URL: http://cce.mitre.org/lists/cce_list.html (дата посл. обращения: 25.03.2014).