МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
(наименование института, филиала)

Кафедра КБ-2«Прикладные информационные технологии»
(наименование кафедры)

ПРАКТИЧЕСКАЯ РАБОТА

по дисциплине: «Основы информационной безопасности»

Обзор стандартов. Работа с содержанием стандартов
(задание)

Задание получил:

_1_ курс, группа _БИСО-02-23_ __23Б0667__
Шифр

_____Макаревич Сергей В._____
ФИО

Проверил:

«__»_____2023 г. _____
Дата *Подпись*

_____ _____
Отметка / результат *ФИО*

Москва 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Была поставлена задача научиться работать с содержанием стандартов. Для этого следует выполнить работу по дисциплине «Основы информационной безопасности».

Цель работы: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

1 Теоретические вопросы

Теоретические вопросы:

1) Предмет и задачи программно-аппаратной защиты информации.

2) Основные понятия программно-аппаратной защиты информации.

3) Классификация методов и средств программно-аппаратной защиты информации.

4) Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

2 Задания

Задания для выполнения:

1. Выписать государственные стандарты в области информационной безопасности.

2. Выписать международные стандарты информационной безопасности.

3. Изучить ГОСТРИСО/МЭК17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

3 Выписать государственные стандарты в области информационной безопасности

Государственные стандарты в области информационной безопасности:

- ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

- ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения

- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества.

- ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

- ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

- ГОСТ Р 52633.1-2009 Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

- ГОСТ Р 52633.2-2010 Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических

образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

- ГОСТ Р 52633.3-2011 Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

- ГОСТ Р 52633.4-2011 Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа.

- ГОСТ Р 52633.5-2011 Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

- ГОСТ Р 52633.6-2012 Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу "Свой".

- ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.

- ГОСТ Р 53109-2008 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.

- ГОСТ Р 53110-2008 Система обеспечения информационной безопасности сети связи общего пользования. Общие положения.

- ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.

- ГОСТ Р 53112-2008 Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.

- ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз

информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

- ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

- ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

- ГОСТ Р 53115-2008 Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.

- ГОСТ Р 53131-2008 Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения.

- ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.

- ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.

- ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.

- ГОСТ Р 56045-2014 Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.

- ГОСТ Р 56093-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования.

- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения.

- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования.

- ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

- ГОСТ Р ИСО 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

- ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.

- ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

- ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

- ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

- ГОСТ Р ИСО/МЭК ТО 15446-2008 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

- ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

- ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

- ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

- ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.

- ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

- ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

- ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.

- ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента

информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

- ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения

- ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

- ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

- ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

- ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1ГОСТ Р ИСО/МЭК 27033-1-2011Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

- ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.

- ГОСТ Р ИСО/МЭК 27034-1-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия

- ГОСТ Р ИСО/МЭК 27037-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

- ГОСТ Р ИСО/МЭК 29100-2013 Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности.

- Рекомендации по стандартизации Р 50.1.050-2004 Защита информации. Система обеспечения качества техники защиты информации. Общие положения.

- Рекомендации по стандартизации Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации

- Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения.

4 Выписать международные стандарты информационной безопасности

Международные стандарты информационной безопасности:

1) COBIT (Основой стандарта являются 40 высокоуровневых целей контроля, сгруппированных в четыре домена, два из которых посвящены информационной безопасности):

- «COBIT 2019 Framework: Introduction and Methodology» — «COBIT 2019 Бизнес-модель: Введение и методология».

- «COBIT 2019 Framework: Governance and Management Objectives» — «COBIT 2019 Бизнес-модель: Задачи руководства и управления.

- «COBIT 2019 DESIGN GUIDE: Designing an Information and Technology Governance Solution — «Проектирование решения по руководству информацией и технологиями».

- «COBIT 2019 IMPLEMENTATION GUIDE: Implementing and Optimizing an Information and Technology Governance Solution» — «Внедрение и оптимизация решения по руководству информацией и технологиями».

2) ITIL и ITSM (Библиотека инфраструктуры информационных технологий или ITIL (The IT Infrastructure Library) — набор публикаций (библиотека), описывающий общие принципы эффективного использования ИТ-сервисов. Библиотека ITIL применяется для практического внедрения подходов IT Service Management (ITSM) — проектирования сервисов и ИТ-инфраструктуры компании, а также обеспечения их связности).

3) ISO

а) Серия ISO/IEC 27XXX (Обращаются в первую очередь при внедрении систем управления ИБ)

Например, самый популярный стандарт ISO/IEC 27001:2013 состоит из двух частей:

- Описание подхода к созданию СУИБ;

- Требования ИБ и средства их реализации, структурированные по разделам.

Стандарт ISO/IEC 27001:2013 имеет российский аналог ГОСТ Р ИСО/МЭК 27001.

б) ISO/IEC 15408 (Содержит единые критерии оценки безопасности ИТ-систем на программно-аппаратном уровне; приводит требования к функциональности средств защиты, которые могут быть использованы при анализе защищённости для оценки полноты реализации функций безопасности; содержит обоснования угроз, политик и требований)

4) NIST (Американская серия стандарта NIST SP 800-XX содержит документы, описывающие подходы к управлению информационной безопасностью, и освещает технические вопросы ее обеспечения (обеспечение безопасности мобильных устройств, защита облачных вычислений, требования к аутентификации, удаленному доступу и т. д.)).

5) SANS. CIS 20 (Руководства CIS Benchmarks — инструмент при настройке или проверке различных элементов ИТ-инфраструктуры на предмет защищенности. Полный перечень включает около 140 наставлений, сгруппированных по разным темам: Desktops & Web Browsers, Mobile Devices, Network Devices, Security Metrics, Servers – Operating Systems, Servers – Other, Virtualization Platforms & Cloud; даёт рекомендации по настройке конфигураций для систем Linux, Windows, MySQL и другие).

6) O-ISM3 (Модель O-ISM3 оперирует четырьмя уровнями управления СУИБ: базовый, стратегический, тактический и операционный. Согласно модели O-ISM3, процессы СУИБ классифицируются по пяти уровням зрелости: Начальный, Управляемый, Описанный, Контролируемый, Оптимизированный).

5 Изучить ГОСТРИСО/МЭК17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами

Требования и рекомендации по защите информации программными и программно-аппаратными средствами*:*

Эти требования касаются инфраструктуры, бизнес-приложений, а также приложений, разработанных пользователями. Процессы проектирования и внедрения бизнес-приложения или сервиса могут быть критичными с точки зрения безопасности. Требования к безопасности следует идентифицировать и согласовывать до разработки информационных систем.

Все требования безопасности, включая необходимые мероприятия по переходу на аварийный режим, следует идентифицировать на стадии определения задач проекта, а также обосновывать, согласовывать и документировать в рамках общего проекта по внедрению информационной системы.

Соответствующие мероприятия по обеспечению информационной безопасности, включая функции аудита или протоколирование действий пользователя, необходимо предусматривать в прикладных системах, включая приложения, написанные самими пользователями. Эти меры должны включать в себя обеспечение функциональности подтверждения корректности ввода, обработки и вывода данных.

Дополнительные мероприятия по обеспечению информационной безопасности могут потребоваться для систем, которые обрабатывают или оказывают воздействие на важные, ценные или критические активы организации, и их необходимо определять на основе требований безопасности и оценки рисков.

5.1 Подтверждение корректности ввода данных

Необходимо обращать особое внимание на корректность входных данных для прикладных систем. При вводе бизнес-транзакций, постоянных данных (имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (цены продаж, курсы валют, ставки налогов) следует применять проверку корректности ввода для обеспечения уверенности в их соответствии исходным данным. Для этого целесообразно применение следующих мероприятий по обеспечению информационной безопасности:

а) проверки исключения двойного ввода или другие проверки ввода с целью обнаружения следующих ошибок:

1) значений, выходящих за допустимый диапазон;

2) недопустимых символов в полях данных;

3) отсутствующие или неполные данные;

4) превышение верхних и нижних пределов объема данных;

5) неавторизованные или противоречивые контрольные данные;

б) периодический анализ (просмотр) содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;

в) сверка твердых (печатных) копий вводимых документов с вводимыми данными на предмет выявления любых неавторизованных изменений этих данных (необходимо, чтобы все изменения во вводимых документах были авторизованы);

г) процедуры реагирования на ошибки, связанные с подтверждением данных;

д) процедуры проверки правдоподобия вводимых данных;

е) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных.

5.2 Контроль обработки данных в системе

5.2.1 Области риска

Данные, которые были введены правильно, могут быть искажены вследствие ошибок обработки или преднамеренных действий. С целью обнаружения подобных искажений в функции систем следует включать требования, обеспечивающие выполнение контрольных проверок. Необходимо, чтобы дизайн приложений обеспечивал уверенность в том, что внедрены ограничения, направленные на минимизацию риска отказов, ведущих к потере целостности данных. Необходимо учитывать, в частности, следующее:

1) Использование места в программах для функций добавления и удаления данных;

2) Процедуры для предотвращения выполнения программ в неправильной последовательности или ее исполнения после сбоя на предыдущем этапе обработки данных;

3) Использование корректирующих программ для восстановления после сбоев и обеспечения правильной обработки данных.

5.2.2 Проверки и средства контроля

Выбор необходимых средств контроля зависит от характера бизнес-приложения и последствий для бизнеса любого искажения данных. Примеры встроенных средств обеспечения информационной безопасности могут быть:

а) средства контроля сеансовой или пакетной обработки с целью выверки контрольных данных (остатков/контрольных сумм) в файлах данных после транзакционных обновлений;

б) средства контроля входящих остатков с целью их проверки с предыдущими закрытыми остатками, а именно:

1) средства контроля "от выполнения - к выполнению";

2) общие суммы измененных данных в файле;

3) средства контроля "от программы - к программе";

в) подтверждение корректности данных, генерированных системой;

г) проверки целостности полученных или переданных данных (программного обеспечения) между центральным (главным) и удаленными компьютерами;

д) контрольные суммы записей и файлов;

е) проверки для обеспечения уверенности в том, что прикладные программы выполняются в нужное время;

ж) проверки для обеспечения уверенности в том, что программы выполняются в правильном порядке и прекращают работу в случае отказа, и что дальнейшая обработка приостанавливается до тех пор, пока проблема не будет разрешена.

5.3 Аутентификация сообщений

Аутентификация сообщений — это метод, используемый для обнаружения неавторизованных изменений или повреждений содержания переданного электронного сообщения. Аутентификация сообщений может быть реализована как аппаратным, так и программным путем в физическом устройстве аутентификации сообщений или в программном алгоритме.

Аутентификацию сообщений необходимо использовать для бизнес-приложений, где должна быть обеспечена защита целостности содержания сообщений, например при электронных переводах денежных средств, пересылке спецификаций, контрактов, коммерческих предложений и прочих документов, имеющих большую важность, или других подобных электронных обменов данными. Чтобы определить, требуется ли аутентификация сообщений, необходимо выполнять оценку рисков безопасности и выбирать наиболее подходящий метод ее реализации.

Аутентификация сообщений не предназначена для защиты содержания сообщения от неправомочного его раскрытия. Для этой цели при аутентификации сообщений могут использоваться криптографические методы.

5.3.1 Подтверждение корректности данных вывода

Данные, выводимые из прикладной системы, необходимо проверять на корректность, чтобы обеспечивать уверенность в том, что обработка информации выполнена правильно. Как правило, системы построены на предпосылке, что при наличии соответствующих подтверждений корректности, проверок и тестирования выводимые данные будут всегда правильны. Но это не всегда так. Подтверждение корректности данных вывода может включать:

1) Проверки на правдоподобие с целью определения, являются ли выходные данные приемлемыми;

2) Проверки контрольных счетчиков на предмет удостоверения, что все данные были обработаны;

3) Обеспечение достаточной информации для получателя результатов вывода или последующей системы обработки, чтобы определить корректность, законченность, точность и классификацию информации;

4) Процедуры по выполнению тестов на подтверждение выводимых данных;

5) Определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных.

5.4 Меры защиты информации, связанные с использованием криптографии

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

5.5 Политика в отношении использования криптографии

Решения относительно применения криптографических мер защиты следует рассматривать в рамках более общего процесса оценки рисков и выбора мероприятий по обеспечению информационной безопасности. Для определения необходимого уровня защиты информации следует проводить оценку рисков, которая должна использоваться для определения того, является ли криптографическое средство подходящим, какой тип средств необходим, с какой целью и в отношении каких бизнес-процессов его следует применять.

В организации следует разработать политику использования криптографических средств защиты информации. Такая политика необходима, чтобы максимизировать преимущества и минимизировать риски, связанные с использованием криптографических средств, а также избежать неадекватного или неправильного их использования. При этом необходимо определить:

а) методику использования криптографических средств в организации, включая общие принципы, в соответствии с которыми следует защищать служебную информацию;

б) принципы управления ключами, включая методы восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей;

в) роли и обязанности должностных лиц за:

1) реализацию политики;

2) управление ключами;

г) соответствующий уровень криптографической защиты для различных данных;

д) перечень мероприятий, которые должны обеспечивать эффективность внедрения методов криптозащиты в организации.

5.6 Шифрование

Шифрование — это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

На основе оценки рисков необходимо определять требуемый уровень защиты, принимая во внимание тип и качество используемого алгоритма шифрования, а также длину криптографических ключей.

При разработке политики использования криптографических средств необходимо учитывать требования законодательства и ограничения, которые могут применяться в отношении использования криптографических методов в разных странах, а также вопросы, касающиеся объема потока зашифрованной информации, передаваемой через границы государств. Кроме того, следует учитывать требования законодательства в отношении экспорта и импорта криптографических технологий.

Для определения необходимого уровня защиты информации, выбора подходящих средств и методов защиты, которые должны обеспечивать требуемый уровень защиты и реализации безопасных способов управления ключами, целесообразно консультироваться со специалистами. Кроме того, может потребоваться консультация юриста относительно законов и нормативных актов, которые могут быть применимы в случае предполагаемого использования организацией методов и средств шифрования.

5.7 Цифровые подписи

Цифровые подписи обеспечивают защиту аутентификации и целостности электронных документов.

Например, электронные подписи могут использоваться при электронной торговле, где есть необходимость в контроле с целью удостовериться, кто подписал электронный документ, а также проверке, было ли содержание подписанного документа изменено.

Цифровые подписи могут применяться для любой формы документа, обрабатываемого электронным способом, например, при подписи электронных платежей, денежных переводов, контрактов и соглашений. Цифровые подписи могут быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой - для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой имеющий к нему доступ может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Кроме того, очень важна защита целостности открытого ключа, которая обеспечивается при использовании сертификата открытого ключа.

Следует уделять внимание выбору типа и качеству используемого алгоритма подписи, и длине ключей. Необходимо, чтобы криптографические ключи, используемые для цифровых подписей, отличались от тех, которые используются для шифрования.

При использовании цифровых подписей необходимо учитывать требования всех действующих законодательств, определяющих условия, при которых цифровая подпись имеет юридическую силу. Например, при электронной торговле важно знать юридический статус цифровых подписей. Может потребоваться наличие специальных контрактов или других

соглашений, чтобы поддерживать использование цифровых подписей в случаях, когда законодательство в отношении цифровых подписей недостаточно развито. Необходимо воспользоваться консультацией юриста в отношении законов и нормативных актов, которые могут быть применимыми в отношении предполагаемого использования организацией цифровых подписей.

5.8 Сервисы неоспоримости

Сервисы неоспоримости следует использовать там, где может требоваться решать споры о наличии или отсутствии события или действия, например спор по использованию цифровой подписи на электронном контракте или платеже. Данные сервисы могут помочь доказать, имел ли место конкретный случай или действие, например отказ в отсылке инструкции, подписанной цифровой подписью, по электронной почте. Эти сервисы основываются на использовании методов шифрования и цифровой подписи.

5.9 Защита криптографических ключей

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования организацией следующих криптографических методов:

1) Методы в отношении секретных ключей, где две или более стороны совместно используют один и тот же ключ, и этот ключ применяется как для шифрования, так и дешифрования информации. Этот ключ должен храниться

в секрете, так как любой, имеющий доступ к этому ключу, может дешифровать всю информацию, зашифрованную с помощью этого ключа, или ввести неавторизованную информацию;

2) Методы в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами могут использоваться для шифрования и для генерации цифровых подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Способы, процедуры и методы защиты криптографических ключей

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

1) Генерации ключей при использовании различных криптографических систем и различных приложений;

2) Генерации и получения сертификатов открытых ключей;

3) Рассылки ключей предназначенным пользователям, включая инструкции по их активации при получении;

4) Хранения ключей; при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам;

5) Смены или обновления ключей, включая правила порядка и сроков смены ключей;

6) Порядка действий в отношении скомпрометированных ключей;

7) Аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или

пользователь уволился из организации (в этом случае ключи необходимо архивировать);

8) Восстановления ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;

9) Архивирования ключей, например для архивированной или резервной информации;

10) Разрушения ключей;

11) Регистрации и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации необходимо, чтобы ключи имели определенные даты активизации и дезактивации, чтобы их можно было бы использовать в течение ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованной форме для доказательств в суде.

В дополнение к вопросу безопасности управления секретными и личными ключами необходимо учитывать необходимость обеспечения защиты открытых ключей. Существует угроза подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготовлять таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары открытого/секретного ключей, с открытым ключом. Поэтому важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять. Этот процесс обычно выполняется органом сертификации, который должен быть признанной организацией, руководствующейся соответствующими правилами и процедурами информационной безопасности для обеспечения требуемой степени доверия к нему.

Необходимо, чтобы содержание соглашений с внешними поставщиками криптографических средств, например с органом сертификации, включало требования по ответственности, надежности средств и времени реагирования на запросы по их предоставлению.

5.10 Безопасность системных файлов

5.10.1 Контроль программного обеспечения, находящегося в промышленной эксплуатации

Необходимо обеспечивать контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию. Чтобы свести к минимуму риск повреждения систем, находящихся в промышленной эксплуатации, целесообразно использовать следующие мероприятия по обеспечению информационной безопасности:

1) Обновление библиотек программ следует выполнять только назначенному специалисту - библиотекарю при соответствующей авторизации его обязанностей руководством;

2) По возможности, системы, находящиеся в промышленной эксплуатации, должны состоять только из исполнимых программных кодов;

3) Исполняемую программу не следует внедрять в промышленную эксплуатацию до тех пор, пока не получены подтверждения ее успешного тестирования и принятия пользователями, а также не обновлены соответствующие библиотеки исходных текстов программ;

4) Необходимо, чтобы журнал аудита регистрировал все обновления библиотек программ, находящихся в промышленной эксплуатации;

5) Предыдущие версии программного обеспечения следует сохранять для восстановления системы в случае непредвиденных обстоятельств.

6) Необходимо, чтобы программное обеспечение, используемое в промышленной эксплуатации, поддерживалось на уровне, заданном

разработчиком. При любом решении провести обновление до уровня новой версии следует принимать во внимание безопасность данной версии: какие новые функциональные возможности обеспечения информационной безопасности она имеет или имеются ли серьезные проблемы обеспечения безопасности, связанные с этой версией. Целесообразно использовать программные модификации (патчи), если они могут закрыть или снизить угрозы безопасности.

Физический или логический доступ предоставляется поставщикам (разработчикам), по мере необходимости, только для поддержки программного обеспечения при наличии разрешения руководства. При этом действия поставщика (разработчика) должны контролироваться.

5.10.2 Защита тестовых данных

Данные тестирования следует защищать и контролировать. Для осуществления системного и приемочного тестирования требуются существенные объемы тестовых данных, которые максимально приближены к операционным данным. Следует избегать использования баз данных, находящихся в промышленной эксплуатации и содержащих личную информацию. Если такая информация требуется для тестирования, то перед использованием следует удалить личную информацию (деперсонифицировать ее). Для защиты операционных данных, когда они используются для целей тестирования, необходимо применять следующие мероприятия по обеспечению информационной безопасности:

1) Процедуры контроля доступа, применяемые для прикладных систем, находящихся в промышленной эксплуатации, следует также применять и к прикладным системам в среде тестирования;

2) При каждом копировании операционной информации для прикладной системы тестирования предусматривать авторизацию этих действий;

3) После того, как тестирование завершено, операционную информацию следует немедленно удалить из прикладной системы среды тестирования;

4) Копирование и использование операционной информации необходимо регистрировать в журнале аудита.

Контроль доступа к библиотекам исходных текстов программ

Для снижения риска искажения компьютерных программ необходимо обеспечивать строгий контроль доступа к библиотекам исходных текстов программ, для чего:

1) По возможности, исходные библиотеки программ следует хранить отдельно от бизнес-приложений, находящихся в промышленной эксплуатации;

2) Назначать специалиста - библиотекаря программ для каждого бизнес-приложения;

3) Персоналу поддержки информационных технологий не следует предоставлять неограниченный доступ к исходным библиотекам программ;

4) Программы, находящиеся в процессе разработки или текущего обслуживания, не следует хранить в библиотеках с исходными текстами программ, находящихся в промышленной эксплуатации;

5) Обновление библиотек и обеспечение программистов исходными текстами следует осуществлять только назначенному специалисту-библиотекарю после авторизации, полученной от менеджера, отвечающего за поддержку конкретного бизнес-приложения;

6) Листинги программ следует хранить в безопасном месте;

7) Следует вести журнал аудита для всех доступов к исходным библиотекам;

8) Старые версии исходных текстов необходимо архивировать с указанием точных дат и времени, когда они находились в промышленной эксплуатации, вместе со всем программным обеспечением поддержки, управления заданиями, определениями данных и процедурами;

9) Поддержку и копирование исходных библиотек следует проводить под строгим контролем с целью предотвращения внесения неавторизованных изменений.

5.11 Безопасность в процессах разработки и поддержки

Менеджеры, ответственные за прикладные системы, должны быть ответственными и за безопасность среды проектирования или поддержки. Они должны проводить анализ всех предложенных изменений системы и исключать возможность компрометации безопасности как системы, так и среды промышленной эксплуатации.

5.11.1 Процедуры контроля изменений

Чтобы свести к минимуму повреждения информационных систем, следует строго контролировать внедрение изменений - строго придерживаться формализованных процедур обеспечения информационной безопасности; осуществлять контроль за возможной компрометацией самих процедур; программистам, отвечающим за поддержку, предоставлять доступ только к тем частям системы, которые необходимы для их работы; обеспечивать формализацию и одобрение соответствующим руководством всех изменений. Изменения в прикладном программном обеспечении могут повлиять на информационную безопасность используемых бизнес-приложений. Там, где это возможно, следует объединять меры по обеспечению информационной безопасности используемых бизнес-приложений и изменений в прикладных программах. Необходимо, чтобы этот процесс включал:

1) Обеспечение протоколирования согласованных уровней авторизации;

2) Обеспечение уверенности в том, что запросы на изменения исходят от авторизованных соответствующим образом пользователей;

3) Анализ мер информационной безопасности и процедур, обеспечивающих целостность используемых систем;

4) Идентификацию всего программного обеспечения, информации, объектов, баз данных и аппаратных средств, требующих изменений;

5) Получение формализованного одобрения детальных запросов/предложений на изменения перед началом работы;

6) Разрешение внесения изменений в прикладные программы авторизованным пользователем до их непосредственной реализации;

7) Осуществление процесса внедрения изменений в прикладные программы с минимальными отрицательными последствиями для бизнеса;

8) Обеспечение обновления комплекта системной документации после завершения каждого изменения и архивирование или утилизация старой документации;

9) Поддержку контроля версий для всех обновлений программного обеспечения;

10) Регистрацию в журналах аудита всех запросов на изменение;

11) Коррекцию эксплуатационной документации и пользовательских процедур в соответствии с внесенными изменениями;

12) Осуществление процесса внедрения изменений в согласованное время без нарушения затрагиваемых бизнес-процессов.

Во многих организациях используется среда, в которой пользователи тестируют новое программное обеспечение и которая отделена от среды разработки и среды промышленной эксплуатации. При этом обеспечивается возможность контроля нового программного обеспечения и дополнительная защита операционной информации, используемой в процессе тестирования.

5.12 Технический анализ изменений в операционных системах

Периодически возникает необходимость внести изменения в операционные системы, например, установить последнюю поддерживаемую

версию программного обеспечения. В этих случаях необходимо провести анализ и протестировать прикладные системы с целью обеспечения уверенности в том, что не оказывается никакого неблагоприятного воздействия на их функционирование и безопасность. Необходимо, чтобы этот процесс учитывал:

1) Анализ средств контроля бизнес-приложений и процедур целостности, чтобы обеспечивать уверенность в том, что они не были скомпрометированы изменениями в операционной системе;

2) Обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривают анализ и тестирование систем, которые необходимо осуществлять при изменениях в операционной системе;

3) Обеспечение своевременного поступления уведомлений об изменениях в операционной системе для возможности проведения соответствующего анализа их влияния на информационную безопасность перед установкой изменений в операционную систему;

4) Контроль документирования соответствующих изменений в планах обеспечения непрерывности бизнеса.

5.13 Ограничения на внесение изменений в пакеты программ

Модификаций пакетов программ следует избегать. Насколько это возможно и допустимо с практической точки зрения, поставляемые поставщиком пакеты программ следует использовать без внесения изменений. Там, где все-таки необходимо вносить изменения в пакет программ, следует учитывать:

1) Риск компрометации встроенных средств контроля и процесса обеспечения целостности;

2) Необходимость получения согласия поставщика;

3) Возможность получения требуемых изменений от поставщика в виде стандартного обновления программ;

4) Необходимость разработки дополнительных мер поддержки программного обеспечения, если организация в результате внесенных изменений станет ответственной за будущее сопровождение программного обеспечения.

В случае существенных изменений оригинальное программное обеспечение следует сохранять, а изменения следует вносить в четко идентифицированную копию. Все изменения необходимо полностью тестировать и документировать таким образом, чтобы их можно было повторно использовать, при необходимости, для будущих обновлений программного обеспечения.

5.14 Скрытые каналы утечки данных и "троянские" программы

Раскрытие информации через скрытые каналы может происходить косвенными и неавторизованными способами. Этот процесс может быть результатом активации изменений параметров доступа как к защищенным, так и к незащищенным элементам информационной системы, или посредством вложения информации в поток данных. "Троянские" программы предназначены для того, чтобы воздействовать на систему неавторизованным и незаметным способом, при этом данное воздействие осуществляется как на получателя данных, так и на пользователя программы. Скрытые каналы утечки и "троянские" программы редко возникают случайно. Там, где скрытые каналы или "троянские" программы являются проблемой, необходимо применять следующие мероприятия по обеспечению информационной безопасности:

1) Закупку программного обеспечения осуществлять только у доверенного источника;

2) Осуществлять контроль доступа к установленным программам и их модификациям;

3) Использовать программное обеспечение, прошедшее оценку на соответствие требованиям информационной безопасности;

4) Осуществлять проверку исходных текстов программ перед их эксплуатационным применением;

5) По возможности закупать программы в виде исходных текстов с целью их проверки;

6) Использование проверенных сотрудников для работы с ключевыми системами.

5.15 Разработка программного обеспечения с привлечением сторонних организаций

В случаях, когда для разработки программного обеспечения привлекается сторонняя организация, необходимо применять следующие меры обеспечения информационной безопасности:

1) Контроль наличия лицензионных соглашений и определенности в вопросах собственности на программы и соблюдения прав интеллектуальной собственности;

2) Сертификацию качества и правильности выполненных работ;

3) Заключение "escrow" соглашения, предусматривающих депонирование исходного текста на случай невозможности третьей стороны выполнять свои обязательства;

4) Обеспечение прав доступа для аудита с целью проверки качества и точности выполненной работы;

5) Документирование требований к качеству программ в договорной форме;

6) Тестирование перед установкой программ на предмет обнаружения "Троянского коня".

ЗАКЛЮЧЕНИЕ

Изучение справочно-правовой системы и анализ нормативных документов по защите информации позволили успешно приобрести необходимые навыки для компетентного применения соответствующего законодательства в практической работе. Этот опыт способствует повышению профессиональной компетентности в области обеспечения безопасности информации.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Электронные ресурсы:

1) Нормативная база ФСТЕК России: https://fstec.ru/dokumenty/vse-dokumenty/perechni/natsionalnye-standarty

Нормативные документы:

1) ГОСТ Р ИСО/МЭК17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

2) Содержание стандартов (COBIT, ISO, ITIL, ITSM, NIST, SANS. CIS 20, O-ISM3)