Хулоса

Таклиф этилаган ахборот хавфсизлигини баҳолашнинг умумий концептуал модели ички баҳолаш жараёнида қўллашга мўлжалланган баҳолаш мезонларини ва кўрсаткичларини ҳамда улар орасидаги боғлиқликларни аниқлашга ва ахборот хавфсизлигини баҳолашнинг умумий концептуал моделининг декомпозициясида шакллантирилган хусусий концептуал моделлар ахборот тизими компонентлари хавфсизлигининг функционал талаблари хусусидаги билимлар базасини аниқлашга ва инсон омилларининг хавфсизлик функциясини амалга оширишга таъсирини кузатишга имкон беради.

Адабиётлар

1. O‘z DSt ISO/IEC 15408-1:2016: Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот технологиялари хавфсизлигини баҳолаш мезонлари. 1-қисм. Кириш ва умумий модел.
2. O‘z DSt ISO/IEC 15408-2:2016: Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот технологиялари хавфсизлигини баҳолаш мезонлари. 2-қисм.Хавфсизликнинг функционал компоненталари.
3. O‘z DSt ISO/IEC 15408-3:2016: Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот технологиялари хавфсизлигини баҳолаш мезонлари. 3-қисм. Хавфсизликка қўйиладиган ишонч компоненталари.

Халмуратов Омонбой Утамуратович
Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Урганч филиали Ахборот технологиялари кафедраси мудири.

Тел:+998901186425
Эл почта: omonboyx@gmail.com

Khalmuratov O.U.

Conceptual model of estimating of security for information technology

Annotation: This article focuses on building a common and customized conceptual model of information security assessment that incorporates evaluation criteria and interconnectivity in the internal evaluation process of the information system.
Keywords: safety assessment models, human factor, program errors, open doors, conceptual model

УДК 004.046(047)

Муминов Б.Б, Эшанкулов Х.И.

ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УЧЁТА ПРОИЗВОДСТВА МАСЛОЖИРОВОЙ ПРОДУКЦИИ

В данной статье рассмотрены требования к созданию автоматизированных систем для масложировых комбинатов, а также последовательность создания программ автоматизации объектов.

Описаны характеристики автоматизируемого объекта, создание автоматизированных рабочих мест, их виды, описаны свойства, которые должны быть присущи таким рабочим местам. В статье подробно описаны этапы создания автоматизированной системы.

Ключевые слова: *автоматизация, численность персонала, эксплуатация, растительное масло, информационная безопасность ,автоматизированные системы.*

Введение Разработка информационной системы должна выполнятся с учетом требований интеграции с системами Электронного правительства. Система должна учитывать требования текущих законодательных и нормативных документов, определяющих правовые основы функционирования рынка маслоэкстракционного производства.

В соответствии с идеологией, Система должна быть выполнена с использованием трехуровневой **архитектуры**.

В целом Система должна обеспечивать работу пользователей в режиме и выполнение своих функций – 24 часов в день, 7 дней в неделю (24х7). **Система должна включать следующие функциональные подсистемы.** Технологический режим функционирования должен характеризоваться проведением работ по запуску системы или ее обслуживанию. В технологическом режиме система должна обеспечивать возможность проведения следующих работ:

- Техническое обслуживание;
- Модернизацию программного комплекса;
- Устранение аварийных ситуаций.

Система должна переходить в аварийный режим при возникновении нештатной ситуации и невозможности штатной работы. Аварийный режим функционирования Системы должен характеризоваться отказом одного или нескольких компонент

программного и (или) технического обеспечения. Аварийный режим не должен повлиять на финансовые показатели потребителей и поставщиков.

Действия обслуживающего персонала при переходе системы в аварийный режим должны быть описаны в руководстве Администратора системы и в регламенте функционирования системы.

Обязательно ведение журналов инцидентов в электронной форме, а также графиков и журналов проведения плановых профилактических работ.

Основная часть

Характеристика объектов автоматизации.

Рафинация растительного масла бывает как физическая (натуральная), так и химическая (с использованием щелочей). Поскольку при производстве масла используются физические методы, на них мы и остановимся. Итак, как правило, физическая рафинация состоит из следующих стадий: гидратация, отбеливание, вымораживание (она же винтеризация) и дезодорация. Гидратация - это удаление из масла фосфолипидов. Именно из-за них нерафинированное масло при жарке дымит, а еда приобретает неприятный вкус и резкий запах удаление фосфолипидов происходит с помощью горячей воды . Для отбеливания, то есть осветления, используется отбельная глина природного происхождения. При этом из масла при удаляются не только пигменты и красящие вещества, но еще и всякие тяжелые металлы и пестициды. Далее происходит удаление восков (парафинов) путем длительного охлаждения масла с последующей фильтрацией.

Воскообразные вещества изначально покрывают семена подсолнечника, защищая их от намокания, пересыхания, но именно они делают масло мутным. И, наконец, необходимо удалить из масла нежелательные продукты окисления и кодирующие вещества, непосредственно влияющие на вкус и запах. В основе процесса дезодорации лежит отгонка (дистилляция) упомянутых ароматических веществ с водяным паром. Для лучшего эффекта данный процесс осуществляют под глубоким вакуумом и при высокой температуре.

Но сначала на завод поступает сырьё. С каждого грузовика в обязательном порядке берется проба для экспертизы в лаборатории. Качество подсолнечного масла напрямую зависит от качества семян подсолнечника, поступающих на переработку, а так же сроков и условий хранения семян перед отжимом. Основными качественными характеристиками для подсолнечных семян являются масличность, сорность, влажность и зараженность вредителями.

Далее грузовик отправляется на разгрузку, где его буквально опрокидывают и семена высыпаются из кузова в специальный бункер.

После разгрузки все семена принятые на завод проходят очистку от сора на сепараторах и при необходимости поступают на сушилку для удаления влаги. После этих операций семена отправляются на хранение. Хранят принимаемое сырье в вентилируемых силосах.

Они бывают на плоском днище и на конусном. В состав силосохранилища входят система вентиляции, система термометрии и система выгрузки.

Вентилируемые силоса на конусном днище. В таких силосах выгрузка семян происходит под действием гравитационных сил.

В прессовом цеху происходит обрушивание семян с последующем отделением ядра от лузги. Лузга направляется в котельную для выработки пара, который потом используется во всем производстве. После влаготепловой обработки ядро направляется на пресса для отжима масла. Кстати, в процессе производства масла прессованием используются мягкие режимы влаготепловой обработки ядра (мезги) - в жаровнях ниже 90°С, что позволяет выпускать масло с более низким перекисным и кислотным числом, чем в традиционных процессах производства (105°С). Прессовое масло после фильтрации направляется на хранение, а полученный после отжима масла жмых подаётся в маслоэкстракционный цех. Там происходит более глубокое извлечение масла из жмыха с помощью специального высокотехнологичного экстрактора.

Экстрагирование масла производится при помощи органических растворителей, в результате чего получается, собственно, раствор масла в растворителе (так называемая мисцелла) и обезжиренный твёрдый остаток (шрот). Далее на стадии дистилляции практически полностью выпариванием удаляется растворитель и полученное масло отправляется на хранение. И, наконец, после экстракционного и прессового цехов полученный продукт отправляют на последующую очистку или рафинацию.

Готовые бутылки транспортер увозит на следующий этап.

Там машина розлива (т.н. филер) наполняет их первоклассным маслом и укупоривает.

Далее бутылки с маслом всё так же автоматически укладываются в коробки. И так же по транспортеру попадают на склад готовой продукции. Коробки укладывают в паллеты и расставляют по стеллажам. Количество устанавливаемого оборудования определяется индивидуально для каждого МЭЗ на этапе формирования технического проекта.

Требования к численности и квалификации персонала системы и режиму его работы.

Весь персонал, участвующий в функционировании системы, условно может быть разделён на следующие группы:

- пользователи системы – сотрудники, обеспечивающие технологический процесс функционирования системы, в соответствии с предоставляемыми правами доступа к данным;
- администраторы системы - выделенный персонал, в обязанности которого входит администриро-

вание системы, обеспечение функционирования Системы и взаимодействия подсистем Системы.

С учетом выполняемой роли в Системе к этим группам персонала предъявляются различные требования, без выполнения которых невозможно обеспечить ее надлежащее функционирование.

Требования к численности персонала. Численность эксплуатирующего персонала автоматизированных рабочих мест Системы должна быть установлена с учётом соблюдения режима работы маслозавода. При этом численность персонала должна быть достаточна для выполнения требуемых функций.

Численность инженерного обслуживающего персонала (в том числе администраторов, технологов, IT-специалистов) должна обеспечивать кругло-суточное поддержание Системы в рабочем состоянии, анализ поступающей информации, постоянную работу по совершенствованию алгоритмов управления на основе полученной информации.

Требования к квалификации персонала. Квалификация персонала должна обеспечивать эффективное функционирование Системы во всех заданных режимах. Персонал должен быть подготовлен к выполнению своих обязанностей в соответствии с должностными инструкциями.

К квалификации персонала должны предъявляться следующие требования.

Администратор баз данных – должен обеспечивать функционирование программных средств системы, сохранность данных системы, его квалификация должна позволять:

- свободно ориентироваться в программно-технической документации;
- свободно ориентироваться в стандартных возможностях используемых ОС и СУБД (реляционных и не реляционных), протоколах передачи данных;
- владеть средствами мониторинга СУБД;
- владеть средствами резервного копирования и восстановления данных;
- работать с архиваторами, дисковыми утилитами, антивирусными программами;
- определять источник сбоя функционирования ПО и производить его описание;
- владеть навыками программирования на языке высокого уровня;
- владеть знаниями и навыками администрирования сетевых инструментов.

Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств.

Администратор информационной безопасности данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по обеспечению информационной безопасности. При этом роли системного администратора, администратора баз данных и администратора информационной безопасности не могут быть совмещены в одну роль.

Пользователь системы – должен обладать навыками работы на персональном компьютере на уровне опытного пользователя и обеспечивать технологический процесс функционирования системы.

В его функциональные обязанности должно входить:

- ввод и контроль информации из документов, файлов;
- формирование запросов и получение информации из системы;
- формирование и вывод выходных документов и материалов.

Его квалификация должна позволять:

- ориентироваться в основных бизнес-процессах автоматизируемой деятельности;
- ориентироваться в основных типах входных и выходных документов и материалов;
- выполнять стандартные процедуры в диалоговой среде, используемой ОС;
- выполнять стандартные процедуры, определенные в системе для ввода исходной информации, получения информации, подготовки выходных форм;
- пользоваться функциями офис-ных приложений, например, таких как MSOffice, Open Office;
- пользоваться различными видами офисной оргтехники. Пользователи Системы должны быть обучены действию во внештатных ситуациях, выхода из строя или сбоя отдельных функций ПО.

Требования к режимам работы персонала

Персонал, работающий с Системой и выполняющий функции её сопровождения и обслуживания, должен работать в следующих режимах:

- Конечный пользователь - в соответствие с основным рабочим графи-ком подразделений Заказчика;
- Администратор баз данных – в соответствие с регламентом функционирования системы и основным рабочим графиком подразделений заказчика.

Требования к приспособляемости системы к изменениям

Программное обеспечение должно иметь высокую гибкость, обеспечивающую расширение функциональных возможностей системы.

Гибкость системы должна определяться способностью допускать включение новых признаков, объектов без разрушения структуры. Необходимая гибкость должна определяться временем жизни системы. Технические решения, принимаемые при модернизации (доработке) Должны использоваться решения, позволяющие обеспечить дальнейшее развитие Системы без ее кардинальной переработки за счет:

- применения современных технологий интеграции;

•наращивания вычислительной мощности технических средств;

•использования сетевого оборудования с более высокой производительностью и других подобных мер. Должны быть определены необходимые границы обеспечения гибкости и настраиваемости системы:

•ввода данных (клиентские приложения);

•базовых механизмов (расчета начислений, формирования счетов и т.п.);

•технологического цикла;

•отдельных технологических операций;

•отчетов;

•загрузок и выгрузок;

•связи с другими системами.

Должна быть предусмотрена возможность масштабирования Системы при увеличении нагрузки на Систему, т.е. должны учитываться требования к увеличению нагрузки, объемов информации и числа пользователей, после-дующему расширению функциональности.

Должна быть предусмотрена возможность расширения и развития функционала системы за счет внедрения новых или модернизации существующих функций системы.

Обеспечение приспособляемости системы должно выполняться за счет:

•своевременности администрирования;

•модификации процедур доступа и представления данных конечным пользователям;

•наличия настроечных и конфигурационных файлов в ПО подсистем.

Требования к надежности

Требования к мероприятиям по обеспечению надежности

Надежность Системы должна достигаться комплексом организационных и технических мер.

Технические меры по обеспечению надежности должны предусматривать:

•резервирование критически важных компонентов и данных системы и отсутствие единой точки отказа;

•использование технических средств с избыточными компонентами и возможностью их «горячей» замены;

•конфигурирование используемых средств в целях повышения надежности

Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок пользователей и обслуживающего персонала, а также минимизацию времени восстановления работоспособности системы за счёт:

•обеспечения требуемого уровня квалификации обслуживающего персонала;

•регламентации, нормативного обеспечения и контроля выполнения работ обслуживающего персонала;

•своевременного оповещения пользователей о случаях нештатной ра-боты компонентов системы;

•обеспечения и контроля работ по сервисному обслуживанию и поддержке компонентов комплекса технических средств, или поддержки собственными специалистами.

Состав показателей надежности для системы в целом

Уровень надежности должен достигаться согласованным применением организационных, организационно технических мероприятий и программно-аппаратных средств.

Надежность должна обеспечиваться за счет:

•применения технических средств, системного и базового программного обеспечения, соответствующих классу решаемых задач;

•своевременного выполнения процессов администрирования системы;

•соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;

•предварительного обучения пользователей и обслуживающего персонала. Время устранения отказа должно быть следующим:

•при перерыве и выходе за установленные пределы параметров электро-питания - не более 45 минут;

•при перерыве и выходе за установленные пределы параметров программного обеспечения - не более 24 часов;

•при выходе из строя АПК Системы - не более 1 часа.

Перечень аварийных ситуаций, по которым регламентируются требования к надежности системы

Под аварийной ситуацией понимается аварийное завершение процесса, выполняемого той или иной компонентой системы, а также «зависание» этого процесса.

При работе Системы возможны следующие аварийные ситуации, которые влияют на надежность работы системы:

•сбой в электроснабжении сервера;

•сбой в электроснабжении рабочей станции пользователей системы;

•сбой в электроснабжении обеспечения локальной сети (поломка сети);

•ошибки Системы, не выявленные при отладке и испытании Системы;

•сбои программного обеспечения сервера.

Требования к надежности программного обеспечения

Система должна обеспечивать возможность резервирования системных и хранимых данных на внешние носители данных и ленточные массивы, а также возможность восстановления данных с внешнего носителя в течение установленного временного интервала.

Контроль безотказного функционирования тех-

нических средств, обнаружение и локализация отказов функционирования.

Система должна обеспечивать защиту от ошибочных действий пользователей, приводящих к аварийному состоянию объекта или системы и ввода некорректных данных.

Компоненты программного обеспечения не должны нарушать целостности друг друга.

Система должна обеспечивать высокий уровень доступности, составляющий не менее 95% в год.

Система должна удовлетворять следующим требованиям к надежности:

•допустимое время штатных простоев Системы при проведении технического обслуживания не должно превышать 32 часов за год;

•допустимое время внештатных простоев системы, возникающих в связи с неисправностью, не должно превышать 24 часов за год;

•допустимое время восстановления системных данных, в случае внештатного простоя системы должно быть указано в регламентной документации;

•допустимое время восстановления хранимых данных, в случае внештатного простоя системы должно быть указано в регламентной документации.

Требования к эргономике и технической эстетике

Эргономичность Системы в части взаимодействия «человек-машина» должны удовлетворять требованиям следующих действующих стандартов:

•ИСО 9241-210-2012 «Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем»;

•ГОСТ 20.39.108-85 «Комплексная система общих технических требований. Требования по эргономике, обитаемости и технической эстетике. Номенклатура и порядок выбора»;

•ГОСТ 12.2.032-78 «Система стандартов безопасности труда. Рабочее место при выполнении работ сидя. Общие эргономические требования»;

•ГОСТ 22269-76 «Система «Чело-век-машина». Рабочее место оператора. Взаимное расположение элементов рабочего места. Общие эргономические требования».

Интерфейс Системы должен соответствовать эргономическим требованиям и обеспечивать доступ к основным функциям и операциям.

Интерфейс должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм и рассчитан на преимущественное использование манипулятора типа «мышь», управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и других элементов.

Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке. Экранные формы должны проектироваться с учетом требований унификации:

•все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;

•для обозначения одних и тех же операций должны использоваться одинаковые графические значки, кнопки и другие управляющие (навигационные) элементы;

•должны быть унифицированы термины, используемые для описания идентичных понятий, операций и действий пользователя;

•реакция Системы на действия пользователя (наведение указателя «мыши», переключение фокуса, нажатие кнопки) должна быть типовой для каждого действия над одними и теми же графическими элементами, независимо от их расположения на экране.

В Системе должна быть реализована система помощи пользователю (контекстные подсказки, справка, ссылка на рабочую документацию и т.д.). Система должна обеспечивать корректную обработку аварийных-ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, пред-шествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Требования к эксплуатации и диагностированию компонентов системы

Система должна обеспечивать реализацию основных функций по рас-чету начислений за жилищно-коммунальные и прочие услуги и мер-социальной поддержки.

Компоненты и подсистемы в процессе функционирования должны находиться в постоянной по времени синхронизации и осуществлять обмен информацией на основе принятых форматов обмена данными.

В случае изменения законодательства и нормативно-правовых актов до ввода системы в действие, в систему и проектную документацию вносятся соответствующие изменения.

В процессе эксплуатации должна быть обеспечена непрерывная работа пользователей в Системе (без технологических пауз), в том числе, работы бухгалтеров Управляющих Организаций и администраторов районов и сотрудников маслозаводов.

Система должна обладать возможностью отката технологических операций. В процессе эксплуатации ограничение доступа пользователей к системе допустимо в период проведения технологических операций. Время проведения технологических операций должно быть определено в регламенте работы Системы, соблюдение которого распространяется на

всех пользователей.

Диагностирование должно осуществляться на уровне функционального ПО, программных и технических комплексов, а также отдельных технических средств.

Система должна предоставлять инструменты автоматического диагностирования основных процессов системы, а также функционирования оборудования и программного обеспечения на основе обработки и анализа поступающей информации.

Система должна предоставлять интерфейс для возможности просмотра диагностических событий, включая события по действиям пользователей и мониторинга процесса выполнения программ, а также проверку доступности смежных и внешних информационных систем.

При возникновении аварийных ситуаций, либо ошибок в программном обеспечении, система должна информировать администратора баз данных посредством вывода информационных сообщений через пользовательский интерфейс или на электронную почту.

При возникновении аварийных ситуаций, либо ошибок в программном обеспечении, диагностические инструменты должны позволять сохранять полный набор информации, необходимой для идентификации проблемы.

Информация о неисправностях должна быть дифференцированной с указанием возможных причин неисправности.

Диагностика аппаратных средств и общесистемного ПО должна быть обеспечена средствами операционной системы и средствами СУБД, либо специализированного ПО.

В части диагностики программного комплекса подсистема комплексного диагностирования Системы должна обеспечивать выполнение следующих функций:

•диагностика специализированного программного обеспечения АС;

•диагностика серверного оборудо-вания АС;

•диагностика компонентов системы.

Результаты диагностики должны быть документированы. Должны быть разработаны регламенты/инструкции по устранению сбоев и неисправностей, которые должны быть представлены в рабочей документации.

Требования к защите информации от несанкционированного доступа, информационной безопасности

Обеспечение информационной безопасности должно формироваться из взаимоувязанного набора наложенных и встроенных средств защиты информации компонент Системы, комплекса организационно-технических мероприятий по обеспечению информационной безопасности в целом, сцелью обеспечить парирование угроз безопасности информации.

Идентификация и аутентификация субъектов доступа и объектов доступа(ИАФ)

Идентификация и аутентификация пользователей, являющихся работниками оператора.

Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных.

Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.

Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Защита обратной связи при вводе аутентификационной информации.

Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

Управление доступом субъектов доступа к объектам доступа(УПД)

Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.

Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

Разделение полномочий (ролей) как для разных категорий пользователей информационной системы, так и внутри категорий, в соответствии с полномочиями.

Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы:

•отнесение пользователей к той или иной категории;

•назначение ролей, групп и прав доступа пользователей. Отображение доступных разделов/функций системы для пользователя в соответствии с правами, которыми он наделён.

Документирование действий пользователей, включая регистрацию:

•имени пользователя при входе в Систему;

•даты и времени сеанса работы (начало/конец);

•фактов добавления, редактирования, исключения данных;

•выполнения пакетных заданий и т.д. Документирование действий пользвателей должно регистрироваться в файле журнала (лог-файле).

Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе), с последующим оперативным оповещнием администратора безопасности при несколь-

ких последовательных неудачных попытках входа в систему.

Формирование «сводок» по доступу пользователей к защищаемым ресурсам. Доступ к данной функции должен быть предоставлен специальной роли – администратору информационной безопасности.

Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.

Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

Протоколы аудита должны быть защищены от несанкционированного доступа как локально, так и в архиве.

Информация, передаваемая по открытым каналам связи (сеть Интернет), должна быть защищена от несанкционированного доступа, т.е. от угроз нарушения ее конфиденциальности и целостности.

Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы). Обеспечение доверенной загрузки средств вычислительной техники.

Ограничение программной среды (ОПС)

Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения.

Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

Защита машинных носителей информации (ЗНИ)

Учет машинных носителей ин-формации. Управление доступом к машинным носителям информации.

Контроль использования интер-фейсов ввода (вывода) информации на машинные носители информации.

Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания).

Регистрация событий безопасности (РСБ)

Определение событий безопасности, подлежащих регистрации, и сроковых хранения.

Определение состава и содержания информации о событиях безопасности, подлежащих регистрации. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора ин-формации и достижение предела или переполнения объема (емкости) памяти. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Генерирование временных меток и (или) синхронизация системного времени в информационной системе. Защита информации о событиях безопасности. Обеспечение возможности просмотра и анализа информации о действиях от-дельных пользователей в информационной системе.

Контроль (анализ) защищенности информации (АНЗ)

Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей.

Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

Контроль работоспособности, пара-метров настройки и правильности функционирования программного обеспечения и средств защиты информации.

Контроль состава технических средств, программного обеспечения и средств защиты информации.

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

Защищённая часть Системы должна использовать "слепые" пароли (при наборе пароля его символы не показываются на экране либо заменяются одним типом символов; количество символов не соответствует длине пароля).

Обеспечение целостности информационной системы и информации (ОЦЛ)

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Защита среды виртуализации (ЗСВ)

Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин. Регистрация событий безопасности в виртуальной инфраструктуре.

Управление (фильтрация, маршрутизация, кон-

троль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

Контроль целостности виртуальной инфраструктуры и ее конфигураций. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфра-структуры. Реализация и управление антивирусной защитой в виртуальной инфраструктуре. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы.

Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.

Исключение возможности отрицания пользователем факта отправки информации другому пользователю. Исключение возможность отрицания пользователем факта получения информации от другого пользователя.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.

Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.

Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы. Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно телекоммуникационными сетями.

Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.

Разграничения ответственности ролей при доступе к компонентам и объектам системы

Состав ролей и определение прав и правил предоставления доступа к компонентам и объектам Системы разрабатывается на этапе технического проектирования.

Требования по сохранности информации при авариях

Должна быть обеспечена сохранность информации в следующих аварийных ситуациях:

- сбой или выход из строя аппаратуры или программного обеспечения;
- сбой или выход из строя коммуникационного оборудования системы;
- аварийное отключение питания.

Для обеспечения сохранности информации в системе должны быть предусмотрены следующие функции:

- настройка параметров резервного копирования компонентов системы с возможностью удаленного хранения;
- управление и учет резервных копий;
- восстановление данных в непротиворечивое состояние при программно-аппаратных сбоях (отключение электрического питания, сбоях операционной Системы и других) вычислительно-операционной среды функционирования;
- восстановление данных в непротиворечивое состояние при сбоях в работе сетевого программного и аппаратного обеспечения.

Защита от ошибочных действий персонала системы должна обеспечиваться с помощью средств управления правами доступа пользователей к информации в соответствии с ролевой моделью.

Для обеспечения восстановления информации, утраченной в результате ошибочных действий уполномоченного персонала, должно быть реализовано циклическое резервное копирование всех данных Системы с сохранением нескольких версий резервных копий.

Для обеспечения высокой доступности и восстановления после аппарат-ных сбоев с минимальными простоями для Системы должно быть использовано решение на базе отказоустойчивого решения, состоящего не менее чем из двух параллельно работающих узлов.

Выход из строя трех жестких дисков дискового массива не должен сказываться на работоспособности подсистемы хранения данных.

Требования к защите от влияния внешних воздействий

Защита от влияния внешних воздействий должна обеспечиваться средствами программно-технического комплекса Заказчика.

Применительно к программно-аппаратному окружению Системы предъявляются следующие требования к защите от влияния внешних воздействий.

Требования к радиоэлектронной защите:

- электромагнитное излучение радио диапазона, возникающее при работе электробытовых приборов, электрических машин и установок, приёмопереда-

ющих устройств, эксплуатируемых на месте размещения АПК Системы, не должны приводить к нарушениям работоспособности подсистем.

Требования по стойкости, устойчивости и прочности к внешним воздействиям:

•Система должна иметь возможность функционирования при колебаниях напряжения электропитания в пределах от 155 до 265 В (220 ± 20% - 30 %);

•Система должна иметь возможность функционирования в диапазоне допустимых температур окружающей среды, установленных изготовителем аппаратных средств.

•Система должна иметь возможность функционирования в диапазоне допустимых значений влажности окружающей среды, установленных изготовителем аппаратных средств.

•Система должна иметь возможность функционирования в диапазоне допустимых значений вибраций, установленных изготовителем аппаратных средств.

Требования по стандартизации и унификации

При создании и модернизации элементов Системы должны использоваться принятые в классификаторы Республики Узбекистан, справочники и словари для различных видов алфавитно-цифровой и текстовой информации.

При создании и модернизации элементов Системы следует руководствоваться действующими национальными стандартами в Республики Узбекистан и другими нормативно-техническими документами.

Используемые оборудование и материалы, подлежащие обязательной сертификации, должны иметь соответствующие сертификаты.

Дополнительные требования

Система должна разрабатываться и эксплуатироваться на аппаратно-техническом комплексе Заказчика.

Необходимо создать отдельные самостоятельные зоны разработки и тестирования компонент Системы.

Для зоны разработки и тестирования должны использоваться те же программные средства, что и для зоны промышленной эксплуатации.

Литературы:

1. ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы (пример) https://www.prj-exp.ru/patterns/pattern_tech_task.php

2. O'zDSt 596:2014. Техникавий шартлар. Семена хлопчатника технические. Технические условия. – Введ. 2014.10.10

3. Круду, Д.Б. Автоматизированная система оперативного мониторинга техно-логических процессов в первичной обработки хлопка-сырца / Д. Б. Круду, А. Ф. Хуайер // Вопросы современной науки: проблемы, тенденции и перспективы : сб. публ. Науч. журнала ―Chronos" по материалам Междунар. науч. – практ. конф. –М : Научный журнал Chronos, 2016. -С. 22 – 25

4. Забегалин Е.В. Технология моделирования архитектуры автоматизированных информационных систем: Сборник методических рекомендаций по определению и моделированию архитектуры автоматизированных информационных систем в консалтинговых проектах. Версия 1.0 / Декабрь 2006 г. / IBS, Департамент управленческого консалтинга.

5. Усков А.А., Кузьмин А.В. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика. М.: Горячая линия - Телеком. 2004. 144с.

6. Anagnostopoulos, Aris, Andrei Z. Broder, and Kunal Pune¬ra. Effective and efficient classification on a search-engine model. 2006. In Proc. CIKM, pp. 208-217. ACM Press. DOI: doi.acm.org/10. 1145/ 1183614. 1183648.

7. Arroso, Luiz André, Jeffrey Dean, and Urs Hölzle. Web search for a planet: The Google cluster architecture. 2003. IEEE Micro 23 (2): 22-28. DOI: dx.doi.org/10.1109/MM.2003.1196112.

Муминов Баходир Болтаевич

Доцент кафедры Мультимедийный технологии Ташкенткого университета информационных технологий имени Мухаммада аль-Хорезми (ТУИТ)

Эл.почта: mbbahodir@gmail.com

Эшонкулов Хамза Илхомович

Старший преподаватель кафедры Информационных технологии Бухарский государственный университета

Эл.почта: khamzaEsh@gmail.com

УДК 551.583

Иброхимов Б.С.

ПРОГНОЗИРОВАНИЕ ИНДЕКСОВ ГЕОМАГНИТНОЙ АКТИВНОСТИ НА ОСНОВЕ ПЕРЕРАСПРЕДЕЛЕНИЯ МАСС СОЛНЕЧНОЙ СИСТЕМЫ

В статье приводятся исследования по индексу геомагнитной активности часового разрешения, что характеризует степень возмущения магнитосферы Земли. Приводится статистический подход по прогностическому моделированию индекса D_{st} часового разрешения без процедур экстраполяции.

Ключевые слова: гравитационные силы, геомагнитный индекс, прогностическая модель, регрессия, адекватность