БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 2 (105). – 48–62

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2022-2-48-62

АНАЛИЗ ОСОБЕННОСТЕЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОПЕРАТИВНОГО ПЛАНИРОВАНИЯ ПРОИЗВОДСТВА*

М.К. СЕРЕБРЕННИКОВ[1], П.В. МИЩЕНКО[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры вычислительной техники. E-mail: serebrennikov.2018@stud.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры вычислительной техники. E-mail: p.mishhenko@corp.nstu.ru*

Информационные системы, используемые предприятиями, обязаны отвечать определенным требованиям безопасности. Система должна быть защищена как от угроз извне, так и от внутренних угроз. Разработчики таких систем должны минимизировать влияние как человеческого фактора, так и различных ошибок и отказов смежных систем на работу разрабатываемой системы. В связи с этим применяются различные техники защиты информационной системы. В работе рассмотрены особенности использования некоторых из них при обеспечении информационной безопасности разрабатываемой автоматизированной системы оперативного планирования производства на одном из действующих предприятий Российской Федерации.

Ключевые слова: Информационная система, автоматизированная система оперативного планирования производства, информационная безопасность, угрозы безопасности

ВВЕДЕНИЕ

Промышленность требует постоянного улучшения методов и инструментов производства для увеличения прибыли. С развитием информационных технологий и их внедрением во все сферы человеческой жизни появилась возможность автоматизации различных производственных процессов. Всё больше предприятий Российской Федерации приобретают различные системы, направленные на автоматизацию множества разных областей и этапов

* Статья получена 20 апреля 2022 г.

производственного процесса [1–14]. При этом любая система, в том числе промышленная, сталкивается с определенными рисками в области информационной безопасности [15]. Угрозы могут быть как внешними, так и внутренними, могут быть связаны с человеческим фактором на производстве или иметь техногенный характер. Реализация любого типа угрозы может привести к остановке производства, к снижению его эффективности или к потере важных данных и, как следствие, к многомиллионным потерям.

Автоматизированная система оперативного планирования производства (АСОПП) не является исключением. Так как эта система является смежной системой по отношению к корпоративным Enterprise Resource Planning (ERP) (система планирования ресурсов предприятия) и Manufacturing Execution System (MES) (система управления производственным процессом) системам, перед ее разработчиками встают проблемы обеспечения безопасной передачи данных между системами, обеспечения надежности разрабатываемой системы и безаварийной работы при отказе смежной системы, защиты информации от несанкционированного доступа и т. д. В связи с этим необходимо проанализировать возможные угрозы информационной безопасности системы, разработать требования к обеспечению ее безопасности и предложить решения возможных проблем.

1. ОПИСАНИЕ АСОПП ПРЕДПРИЯТИЯ

Разрабатываемая АСОПП предприятия предназначена для построения и оперативного изменения производственного расписания при заданном времени и критериях оптимизации, складских остатков сырья, материалов и готовых изделий, загрузки оборудования, графиков ППР, доступности ресурсов, спецификаций, режимов производства и справочной информации.

Структура АСОПП включает следующие компоненты:

- сервер базы данных – виртуальная машина, назначением которой является обеспечение надежного хранения, обработки и предоставления данных системы;
- сервер лицензирования – виртуальная машина, назначением которой является обеспечение функционирования системы только при наличии необходимых лицензий;
- автоматизированные рабочие места (АРМ) – предназначены для организации интерфейса пользователя на рабочих местах персонала.

Сервер базы данных АСОПП будет представлять собой виртуальный сервер, расположенный в единой среде виртуализации на кластере физических серверов, предоставляемом заказчиком.

Производственный процесс на объекте автоматизации разделен на несколько этапов, каждый из которых выполняется в специально выделенном цехе. Соответственно каждый цех будет оборудован своим АРМ.

Смежными системами для системы оперативного планирования производства являются:

- АСУПП (MES) – автоматизированная система управления производственными процессами;
- АСАПД (MI) – система производственной аналитики (система подготовки данных, построения отчетов и дашбордов);
- заводская ERP-система.

Входная информация, необходимая для работы АСОПП, будет приоритетно получаться из АСУПП (при условии, что данная информация имеется в АСУПП). Если АСУПП не будет иметь требуемой информации, то будет выполняться импорт информации в АСОПП из ERP-системы, располагающей такой информацией.

В АСУПП будет загружаться выходная информация АСОПП, кроме информации, передаваемой напрямую в ERP.

Все сообщения будут включать в состав стандартные данные:

- идентификатор сообщения;
- идентификатор источника;
- идентификатор приемника;
- дату и время формирования сообщения в формате UTC.

Взаимодействие АСОПП со смежными подсистемами уровня Manufacturing Operations Management (MOM) будет выполняться через интеграционную шину уровня MOM, которая будет выполнять необходимые преобразования форматов данных и сама по себе не является ни источником, ни приемником данных.

2. АНАЛИЗ ВОЗМОЖНЫХ УГРОЗ

Возможные угрозы информационной безопасности для АСОПП предприятия могут относиться к следующим видам:

- уничтожение или искажение информации;
- раскрытие конфиденциальной информации;
- неправомерное вмешательство в работу компьютерной системы;
- вывод компьютерной системы из строя, снижение ее работоспособности;
- превышение полномочий непривилегированных пользователей;
- отказ от авторства и транзакций.

Некоторые из угроз, относящиеся к вышеперечисленным видам, могут реализовываться независимо друг от друга, т. е. наступление последствий одной или нескольких угроз возможно при реализации угрозы другого вида. Так, уничтожение или искажение информации возможно после неправомерного вмешательства в работу системы или при превышении полномочий пользователем.

Для исследования возможных угроз для системы необходимо определиться с классификацией угроз. Здесь будут рассмотрены угрозы с классификацией по происхождению и по месту возникновения.

Уничтожение или искажение информации может относиться к внешней угрозе при реализации взлома извне и в таком случае будет иметь антропогенный характер. Эта угроза будет являться внутренней в случае, если произошел сбой в работе самой системы либо в работе смежной системы. В этом случае угроза будет классифицирована как техногенная. Антропогенная классификация для внутренней угрозы данного вида применима в случае, если деструктивные действия были совершены со стороны пользователей системы намеренно (саботаж) или не намеренно (недостаточная квалификация для работы с системой).

Раскрытие конфиденциальной информации для предприятия, которому разрабатывается АСОПП, будет являться внешней угрозой, так как ущерб от ее раскрытия будет заключаться в утечке информации за пределы этой организации. Если утечка произойдет при работе какого-либо компонента системы (например, при ошибочной отправке сообщения с данными клиенту, находящемуся за пределами предприятия), то эта угроза будет классифицирована как техногенная. Если утечка произойдет по вине сотрудника предприятия, угроза будет антропогенной.

Неправомерное вмешательство в работу системы (взлом) может быть внешней угрозой, если реализуется хакером за пределами организации, и внутренней, если сотрудник, не имеющий допуска к работе с АРМ системы, получит к нему доступ. В перечисленных случаях угроза носит антропогенный характер.

Вывод компьютерной системы из строя или снижение ее работоспособности может являться целью взлома, при осуществлении взлома извне эта угроза будет являться внешней. В остальных случаях она будет классифицирована как внутренняя. При этом отказ системы может быть вызван исключительной ситуацией, произошедшей из-за внутренней ошибки алгоритмов одного или нескольких компонентов системы, тогда угроза является техногенной. В случае отказа по вине пользователя (например, при вводе неверной комбинации данных или нарушении алгоритма работы с программным комплексом системы) угроза будет являться антропогенной.

Повреждение аппаратной части системы также может носить как антропогенный, так и техногенный характер.

Превышение полномочий непривилегированных пользователей может возникнуть, например, в случае, если пользователь, который должен иметь доступ только к просмотру производственного расписания, построенного АСОПП, внесет в него изменения или уничтожит его. Эта угроза является антропогенной и внутренней.

Отказ от авторства и транзакций может возникнуть после передачи справочной информации от ERPили АСУПП, после передачи информации между клиентами АСОПП либо после передачи информации, относящейся к построенному календарному плану от АСОПП в АСУПП. При штатном функционировании систем данная угроза может иметь только внутренний антропогенный характер. Сбой в работе какой-либо из смежных систем, позволяющий классифицировать угрозу как техногенную, может произойти только при ошибке в адресации сообщений между системами. Так, подсистема АСОПП, осуществляющая среднесрочное планирование при формировании сообщения к подсистеме краткосрочного планирования одного из цехов, может заполнить в поле, идентифицирующем отправителя, данные о какой-либо другой подсистеме.

3. РЕШЕНИЯ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСОПП ПРЕДПРИЯТИЯ

Решения проблем информационной безопасности АСОПП предприятия зависят от классификации угрозы. Так, большинство внешних угроз будет решено изоляцией корпоративной сети, в которой будут функционировать АСОПП предприятия и системы, смежные с ней. Сеть предприятия не имеет выхода в Интернет, что позволяет отсечь угрозу внешнего взлома и все угрозы, связанные с ней. Также изоляция делает невозможным распространение конфиденциальной информации посредством отправки через Интернет. Отсюда следует требование к АСОПП: система не должна требовать доступа к глобальной сети, должна ограничиваться только корпоративной сетью. Это требование будет выполнено посредством размещения всей необходимой инфраструктуры в пределах предприятия. Например, на специально выделенном на территории завода серверном оборудовании будет развернут сервер лицензирования и прочие необходимые для работы системы компоненты.

При изоляции корпоративной сети для неправомерного вмешательства в работу системы остается только вариант внутренней реализации угрозы. В связи с этим к АСОПП выдвигаются требования к функциям и режиму ра-

боты персонала, к эксплуатации и хранению, к защите информации от несанкционированного доступа. Для обеспечения эксплуатации системы оперативного планирования производства в составе служб будут выделены следующие роли:

- системный администратор;
- пользователь;
- администратор приложения (с функцией администратора баз данных).

Системный администратор будет выполнять следующие функции:

- установка, обновление и мониторинг программного обеспечения (ПО);
- устранение неисправностей функционирования ПО и комплекса технических средств;
- ведение учетных записей пользователей;
- выполнение функций по резервному копированию данных.

Пользователь при работе с системой будет выполнять следующие основные функции:

- построение производственного расписания;
- корректировка и изменения построенного системой расписания;
- просмотр и контроль полученных данных в виде диаграммы Ганта и отчетов;
- формирование отчетов на основе имеющихся шаблонов отчетов и исходных данных.

Администратор приложения, помимо основных функций пользователя, будет выполнять следующие функции:

- проверка корректности работы ПО;
- первичная диагностика некорректной работы ПО;
- осуществление поддержки пользователей при работе с системой (администратор должен иметь представление о функциональности системы);
- разграничение прав пользователей в системе в зависимости от назначенной ему роли;
- администрирование баз данных.

Деятельность сотрудников, эксплуатирующих систему, будет регламентироваться должностными инструкциями и основным рабочим графиком подразделений производства.

Размещение помещений и оборудования будет исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

Защита информации от несанкционированного доступа будет обеспечивать:

- идентификацию пользователей при помощи стандартной процедуры «логин–пароль»;
- разграничение доступа. Пользователям системы будут назначаться права доступа в рамках их должностных обязанностей.

Выполнение приведенных требований решает также проблему превышения полномочий непривилегированных пользователей. Аппаратные средства (считыватели смарт-карт), интегрируемые в терминалы АРМ, позволят использовать электронный пропуск сотрудника в качестве ключа к терминалу. Так как доступ на предприятие предоставляется только сотрудникам предприятия, при этом каждый сотрудник имеет электронный пропуск и может быть однозначно идентифицирован, это исключает ошибочное использование АРМ системы сотрудником, не имеющим к нему допуска.

Минимизация угроз, имеющих антропогенный характер, связанных с непреднамеренными деструктивными действиями, такими как уничтожение, искажение информации или нарушение порядка работы с АРМ системы, будет достигнута выполнением требований к квалификации персонала, к эргономике и технической эстетике и требований по стандартизации и унификации интерфейсных форм.

Все пользователи системы должны будут обладать следующими знаниями:

- знанием предметной области планирования производства;
- знанием используемого общесистемного программного обеспечения;
- знанием методики и приемов работы в программных компонентах системы;
- знанием методики и приемов внедренческой работы.

Для обслуживания системы будет назначен сотрудник, выполняющий роль администратора приложения. Допускается совмещение функций администрирования АСОПП и смежных информационных систем.

Основные задачи, выполняемые администратором приложения:

- техническая поддержка пользователей;
- взаимодействие со службой технической поддержки вендора;
- выполнение регламентных мероприятий по обслуживанию системы и обеспечению ее отказоустойчивости.

Администратор приложения дополнительно должен будет обладать навыками администрирования ОС Windows и СУБД MS SQL Server, а также уметь разрабатывать запросы на языке Transact-SQL.

АСОПП будет иметь русифицированный интерфейс (за исключением системной части) на всех стадиях ввода, обработки, анализа и передачи информации, позволяющий пользователю свободно ориентироваться в информационном наполнении и функциональном применении.

Экранные формы пользовательского интерфейса системы будут разработаны с учетом современных требований по эргономике и технической эстетике. К числу таких требований относятся следующие:

- взаимодействие пользователей посредством визуального графического интерфейса;
- пункты меню в пользовательских интерфейсах должны быть сгруппированы в соответствии с тематикой информации, функциональными задачами и технологией работы;
- пункты меню должны называться или изображаться так, чтобы пользователь однозначно понимал их назначение;
- для облегчения восприятия информации, отображаемой в пользовательских интерфейсах, должна быть реализована система цветовых индикаторов в зависимости от статуса / состояния объектов;
- цветовое решение интерфейса должно быть выдержано в спокойных тонах, не вызывающих утомления зрения;
- задание критериев для выполнения поиска и выборки информации без задействования языков программирования;
- наличие оптимального набора используемых словарей и справочников;
- клавиатурный режим ввода должен использоваться, главным образом, при заполнении и редактировании текстовых и числовых полей экранных форм;
- с технологической точки зрения пользовательский интерфейс программного обеспечения должен выполняться в виде набора взаимосвязанных форм и средств навигации.

Интерфейсные формы системы будут спроектированы с учетом следующих требований унификации:

- все формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
- в разделах интерфейса для обозначения операций, приводящих к одному и тому же результату (сохранение информации, отправка, печать), должны использоваться одинаковые графические значки, кнопки и другие управляющие и навигационные элементы;
- термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также по-

следовательности действий пользователя при их выполнении, должны быть унифицированы;

- для однотипных графических элементов пользовательского интерфейса должно быть предусмотрено одинаковое поведение в процессе взаимодействия с пользователем (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки);
- ввод–вывод данных, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме, в реальном режиме времени;
- должно быть обеспечено явное подтверждение пользователем сохранения вводимой или изменяемой информации посредством диалога;
- пользовательский интерфейс должен в максимальной степени обеспечивать быстрое исполнение команд за счет:

– использования функциональных или быстрых клавиш;

– использования средств автоматического поиска для выбора необходимых параметров;

– заполнения отдельных реквизитов форм значениями «по умолчанию».

Выполнение вышеперечисленных требований минимизирует риски ошибочного использования функций системы, искажения информации, возникновения исключительных ситуаций вследствие ввода неприемлемой комбинации данных и т. п., так как только квалифицированный пользователь будет работать с системой посредством оптимизированного и удобного интерфейса, все функции и специфика использования которого будут ему понятны.

Угрозы, имеющие техногенный характер, будут минимизированы путем выполнения требований к надежности, к эксплуатации, техническому обслуживанию и ремонту системы, а также требований по сохранности информации при авариях.

Система будет сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- сбои программного обеспечения;
- выход из строя части комплекса технических средств;
- сбои в электроснабжении на рабочем месте пользователя системы или сервера.

После сбоя серверной операционной системы или СУБД в процессе выполнения пользовательских задач будет обеспечено восстановление данных до состояния на момент окончания последней нормально завершенной перед сбоем транзакции.

Надежность системы будет обеспечиваться за счет:

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

- своевременного выполнения процессов администрирования системы;
- ведения журнала событий системы в электронном виде;
- соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;
- предварительного обучения пользователей и обслуживающего персонала.

Периодическое обслуживание используемых технических средств будет проводиться в соответствии с требованиями технической документации разработчика системы, но не реже одного раза в год.

Периодическое обслуживание и тестирование технических средств будет включать в себя обслуживание и тестирование всех используемых средств, включая рабочие станции, серверы, кабельные системы и сетевое оборудование, устройства бесперебойного питания.

В процессе проведения периодического технического обслуживания будет проводиться внешний и внутренний осмотр технических средств, проверка контактных соединений, проверка параметров настроек работоспособности технических средств и тестирование их взаимодействия.

На основе результатов тестирования технических средств будет проводиться анализ причин возникновения обнаруженных дефектов и будут приниматься меры по их ликвидации.

Восстановление работоспособности технических средств будет проводиться в соответствии с инструкциями разработчика и поставщика технических средств и документами по восстановлению работоспособности технических средств и будет завершаться проведением их тестирования. При вводе системы в опытную эксплуатацию будет разработан план выполнения резервного копирования программного обеспечения и обрабатываемой информации. Во время эксплуатации системы персонал, ответственный за эксплуатацию системы, должен будет выполнять разработанный план.

Размещение оборудования и технических средств будет соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

Все пользователи системы должны будут соблюдать правила эксплуатации электронной вычислительной техники, правила эксплуатационной документации на систему. Квалификация персонала и его подготовка должны будут соответствовать технической документации. Для работы с системой пользователь может не обладать навыками программирования.

Программное обеспечение системы будет восстанавливать свое функционирование при корректном перезапуске аппаратных средств. Будет предусмотрена возможность организации автоматического или ручного резервного копирования данных системы средствами системного ПО.

Выполнение требований со стороны разработчиков в реализуемой АСОПП обеспечивается наличием двух типов серверов: базовым и для резервного копирования информации. Также при работе с системой будет использоваться транзакционность, т. е. манипуляции с данными будут проводиться в формате транзакций, что гарантирует завершенность этих действий с данными. Так, при сбое в системе начатые манипуляции с данными не приведут к несогласованности данных и, как следствие, к ошибкам в работе системы.

Проблема отказа от авторства и транзакции будет решена в совокупности с перечисленными выше решениями минимизацией человеческого фактора при передаче данных между смежными системами. Так, при необходимости в обновлении справочных данных АСОПП «по кнопке», т. е. автоматизированно с минимальными требованиями к входным данным от пользователя, будет делать запрос к конкретной подсистеме ERP, получать и автоматически обрабатывать полученные данные в соответствии с заложенным на этапе реализации сценарием импорта. При этом передаваемые данные будут иметь строго определенный на этапе разработки формат. При изменении данных на стороне ERP эта система будет автоматически присылать данные об изменениях в АСОПП, при этом сообщение будет генерироваться системой без участия человека, что исключит возможность подмены данных об отправителе. Такой принцип работы распространяется и на взаимодействие АСОПП с другими смежными системами уровня MES, и на взаимодействие отдельных подсистем АСОПП.

ЗАКЛЮЧЕНИЕ

Несмотря на многообразие угроз информационной безопасности, существует множество способов исключения их реализации или минимизации вероятности наступления их последствий. В настоящей работе рассмотрены лишь некоторые из этих способов на примере реализуемой АСОПП в рамках проекта по модернизации предприятия. Данные способы подходят не только для обеспечения безопасности АСОПП, но и для других систем. Стоит отметить, что тщательный анализ угроз на этапе обследования позволяет выдвинуть наиболее полные требования к системе. Благодаря выполнению этих требований можно максимально обезопасить систему от выявленных уязвимостей, что позволяет избежать значительных убытков и репутационных потерь в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. *Реутов А.П., Черняков М.В., Замуруев С.Н.* Автоматизированные информационные системы: методы построения и исследования. – М.: Радиотехника, 2010. – 328 с.

2. *Вендров А.М.* Современные методы и средства проектирования информационных систем. – М.: Финансы и статистика, 2008. – 65 с.

3. *Ипатова Э.Р., Ипатов Ю.В.* Методологии и технологии системного проектирования информационных систем. – М.: Флинта, 2008. – 256 с.

4. *Маклаков С.В.* Создание информационных систем с All Fusion Modeling Suite. – М.: Диалог-МИФИ, 2007. – 432 с.

5. *Маклаков С.В.* CASE-средства разработки информационных систем. – М.: Диалог-МИФИ, 2007. – 304 с.

6. *Муромцев В.В., Ломазов В.А.* Проектирование информационных систем: учебное пособие для студентов вузов заочной формы обучения по специальности 010502 «Прикладная информатика в экономике». – Белгород: БелГУ, 2007. – 160 с.

7. *Петров В.Н.* Информационные системы. – СПб.: Питер, 2002. – 688 с.

8. *Смирнова Г.Н., Сорокин А.А.* Проектирование экономических информационных систем: учебное пособие. – М.: Высшая школа, 2002. – 428 с.

9. Автоматизированные информационные технологии в экономике: учебник / под ред. Г.А. Титоренко. – М.: Юнити, 2003. – 399 с.

10. *Федоров Н.В.* Проектирование информационных систем на основе современных CASE-технологий: учебное пособие. – М.: Моск. гос. индустр. ун-т, 2008. – 128 с.

11. *Черемных С.В., Семенов И.О., Ручкин В.С.* Структурный анализ систем: IDEF-технологии. – М: Финансы и статистика, 2001. – 208 с.

12. 1С: Предприятие 8. – URL: http://solutions.1c.ru/catalog/wms/ (дата обращения: 02.06.2022).

13. Ресурсы информационных систем. – URL: http://www.economica-upravlenie.ru/content/view/204/ (дата обращения: 02.06.2022).

14. Сертифицированные информационные системы. – URL: http://certsys.ru/products/index.php (дата обращения: 02.06.2022).

15. *Чипига А.Ф.* Информационная безопасность автоматизированных систем. – М.: Гелиос АРВ, 2017. – 336 с.

Серебренников Максим Кириллович, лаборант кафедры вычислительной техники Новосибирского государственного технического университета. E-mail: serebrennikov.2018@stud.nstu.ru

Мищенко Полина Валерьевна, старший преподаватель кафедры вычислительной техники Новосибирского государственного технического университета. Область научных интересов: распределенные вычислительные системы, информационные сети. E-mail: p.mishhenko@corp.nstu.ru

DOI: 10.17212/2782-2230-2022-2-48-62

Analysis of the features of information security ensuring of the automated system of operational production planning*

M.K. Serebrennikov[1], P.V. Mishchenko[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Computer Engineering Department. E-mail: serebrennikov.2018@stud.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the Computer Engineering Department. E-mail: p.mishhenko@corp.nstu.ru*

Information systems used by enterprises meet certain security requirements. The system must be protected from both external and internal threats. Developers of such systems should minimize the impact of both the human factor and various errors and failures of adjacent systems on operation of the system being developed. In this regard, various information system protection techniques are used. The paper considers the features of using some of them in ensuring information security of the automated system of operational production planning being developed at one of the operating enterprises of the Russian Federation.

Keywords: Information system, automated system of operational production planning, information security, security threats

REFERENCES

1. Reutov A.P., Chernyakov M.V., Zamuruev S.N. *Avtomatizirovannye informatsionnye sistemy: metody postroeniya i issledovaniya* [Automated information systems: methods of construction and research]. Moscow, Radiotekhnika Publ., 2010. 328 p.

* *Received 20 April 2022.*

2. Vendrov A.M. *Sovremennye metody i sredstva proektirovaniya informatsionnykh sistem* [Modern methods and tools for designing information systems]. Moscow, Finansy i statistika Publ., 2008. 65 p.

3. Ipatova E.R., Ipatov Yu.V. *Metodologii i tekhnologii sistemnogo proektirovaniya informatsionnykh sistem* [Methodologies and technologies for system design of information systems]. Moscow, Flinta Publ., 2008. 256 p.

4. Maklakov S.V. *Sozdanie informatsionnykh sistem s All Fusion Modeling Suite* [Building information systems with All Fusion Modeling Suite]. Moscow, Dialog-MIFI Publ., 2007. 432 p.

5. Maklakov S.V. *CASE-sredstva razrabotki informatsionnykh sistem* [CASE-tools for developing information systems]. Dialog-MIFI Publ., 2007. 304 p.

6. Muromtsev V.V., Lomazov V.A. *Proektirovanie informatsionnykh sistem* [Designing information systems]. Belgorod, BelGU Publ., 2007. 160 p.

7. Petrov V.N. *Informatsionnye sistemy* [Information systems]. St. Petersburg, Piter Publ., 2002. 688 p.

8. Smirnova G.N., Sorokin A.A. *Proektirovanie ekonomicheskikh informatsionnykh sistem* [Design of economic information systems]. Moscow, Vysshaya shkola Publ., 2002. 428 p.

9. Titorenko G.A., ed. *Avtomatizirovannye informatsionnye tekhnologii v ekonomike* [Automated information technology in the economy]. Moscow, Yuniti Publ., 2003. 399 p.

10. Fedorov N.V. *Proektirovanie informatsionnykh sistem na osnove sovremennykh CASE-tekhnologii* [Designing information systems based on modern CASE-technologies]. Moscow, Moscow State Industrial University Publ., 2008. 128 p.

11 Cheremnykh S.V., Semenov I.O., Ruchkin V.S. *Strukturnyi analiz sistem: IDEF-tekhnologii* [Structural analysis of systems: IDEF-technologies]. Moscow, Finansy i statistika Publ., 2001. 208 p.

12. *1S: Predpriyatie 8*. [1C: Enterprise 8]. Available at: http://solutions.1c.ru/catalog/wms/ (accessed 02.06.2022).

13. Resursy informatsionnykh sistem [Information systems resources]. Available at: http://www.economica-upravlenie.ru/content/view/204/ (accessed 02.06.2022).

14. Sertifitsirovannye informatsionnye sistemy [Certified information systems]. Available at: http://certsys.ru/products/index.php (accessed 02.06.2022).

15. Chipiga A.F. *Informatsionnaya bezopasnost' avtomatizirovannykh sistem* [Information security of automated systems]. Moscow, Gelios ARV Publ., 2017. 336 p.

Для цитирования:

Серебренников М.К., Мищенко П.В. Анализ особенностей обеспечения информационной безопасности автоматизированной системы оперативного планирования производства // Безопасность цифровых технологий. – 2022. – № 2 (105). – С. 48–62. – DOI: 10.17212/2782-2230-2022-2-48-62.

For citation:

Serebrennikov M.K., Mishchenko P.V. Analiz osobennostei obespecheniya informatsionnoi bezopasnosti avtomatizirovannoi sistemy operativnogo planirovaniya proizvodstva [Analysis of the features of information security ensuring of the automated system of operational production planning]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 2 (105), pp. 48–62. DOI: 10.17212/2782-2230-2022-2-48-62.