УДК 004.056

А. Г. ОКСИЮК, Я. В. ШЕСТАК, О. Д. ОГБУ

ПОСТРОЕНИЕ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ КАК НЕОБХОДИМОСТЬ ВЫЖИВАНИЯ

Главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов Заказчика от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта. Другой целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности, имущественных прав и интересов клиентов.

Ключевые слова: система информационной безопасности, информация, угроза, защита, ИТ-инфраструктура.

Головною метою будь-якої системи інформаційної безпеки є забезпечення стійкого функціонування об'єкту, відвертання загроз його безпеки, захист законних інтересів Замовника від протиправних посягань, недопущення розкрадання фінансових коштів, розголошування, втрати, витоку, спотворення і знищення службової інформації, забезпечення нормальної виробничої діяльності усіх підрозділів об'єкту. Іншою метою системи інформаційної безпеки є підвищення якості послуг, що надаються, і гарантій безпеки, майнових прав і інтересів клієнтів.

Ключові слова: система інформаційної безпеки, інформація, загроза, захист, ИТ-інфраструктура.

It is necessary to consider many factors while building a secure information infrastructure. Not all of them are obvious and it is not always possible to predict which exactly security systems it will be necessary to include to the information infrastructure. Structured information presented in this report will help us with this article. In this article, the main points of the establishing of a protected information infrastructure were considered. As statistics show, most incidents occur not occasionally since they are the results of malicious actions of the personnel or their unconscientiousness of how to execute their professional duties of for setting up the information infrastructure.

A lot of information regarding the construction of a secure information infrastructure can be obtained from various documents, such as ISO / IEC 27001, PCI DSS, ISMS, various guidelines such as internal regulations and instructions, explanations to the law of Ukraine on information security. All these documents have many different versions and interpretations. Since there is no single standard for building a secure information infrastructure, there arises a solution to combine all available protection techniques and to develop a generalized model that, when implemented, can be expected to yield acceptable results.

When analyzing the vulnerabilities article in the article, one can see that a sufficiently large amount of work should to be carried out by the IT security service, which should be even more developed than the technical specialists who serve and sustain the information infrastructure system. The main task for information security specialists is not to protect the perimeter from an external enemy and not to protect the information infrastructure from external violators, but to accompany technical specialists and check the actions of technical personnel and only after all of that, to protect the system against external enemy.

A practice shows, more than 80% of all vulnerabilities of the information infrastructure were identified during analyzing the settings of the information infrastructure and the actions of technical personnel. In one banking structure of Ukraine, after using this technique, the number of external attacks was reduced by 90 %, implementation of this technique reduced to "0" the amount of information leaks caused by bank employees. This once again underlines the importance of building a secure information infrastructure using different methods depending on the needs of the business and new directions in the development of information technologies.

Keywords: information security system, information, threat, protection, IT infrastructure.

Вступ. Уровень развития современных технологий позволяет компаниям создавать сложные корпоративные инфраструктуры, объединяющие в себе множество подсистем. Зачастую архитектура сети настолько сложна, что обеспечить ее полную защиту становится непосильной задачей даже для крупных корпораций, выделяющих солидный бюджет на защиту своих ресурсов.

Главной целью любой системы информационной безопасности является построение, такой модели безопасности при которой с одной стороны будет достигнута максимальная защита информационных ресурсов и информации от посягательств третьих лиц, потери информации вследствие действия третьих лиц, или иных воздействий, которые могут привести к неработоспособности информационной системы или потере, краже информации. С другой стороны, будет достигнута максимальная повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Достижение заданных целей возможно в ходе решения следующих основных задач. Рассмотрим перечень основных задач, которые необходимо решить для решения задачи построения защищенной информационной инфраструктуры:

– отнесение информации к категории ограниченного доступа (служебной тайне);

– прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению ущерба, нарушению его нормального функционирования;

– создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения ущерба;

– создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

– создание условий для максимально возможного возмещения и локализации ущерба, ослабление негативного влияния последствий нарушения информационной безопасности.

Достижение заданных целей возможно в ходе решения следующих основных задач:

– отнесение информации к категории ограниченного доступа;

– прогнозирование и своевременное выявление угроз безопасности;

– создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения ущерба;

– создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании;

– создание условий для максимально возможного возмещения и локализации ущерба, ослабление негативного влияния последствий нарушения информационной безопасности.

Задача отнесение информации к категории ограниченного доступа (служебной тайне). Согласно статьям 7–9 закона Украины О доступе к публичной информации делиться на следующие типы:

1. Конфиденциальная информация – информация, доступ к которой ограничен физическим или юридическим лицом, кроме субъектов властных полномочий, и которая может распространяться в определенном ими порядке по их желанию в соответствии с предусмотренными ими условиями. Не может быть отнесена к конфиденциальной информация.

2. Секретная информация. Секретной признается информация, содержащая государственную, профессиональную, банковскую тайну, тайну следствия и иную предусмотренную законом тайну.

Служебная информация в соответствии с требованиями Закона может относиться следующая информация:

1) которая содержится в документах субъектов властных полномочий, представляющих внутриведомственную служебную корреспонденцию, докладные записки, рекомендации, если они связаны с разработкой направления деятельности учреждения или осуществлением контрольных, надзорных функций органами государственной власти, процессом принятия решений и предшествуют публичному обсуждению и/или принятию решений;

2) собранная в процессе оперативно-розыскной, контрразведывательной деятельности, в сфере обороны страны, которая не отнесена к государственной тайне.

К этим типам информации доступ необходимо ограничивать, ко всем остальным типам информации можно и не ограничивать доступ. Исходя из типа информации и функционала разрабатывается и матрица доступа к информации.

Следующий пункт-это прогнозирование и своевременное выявление угроз безопасности информационным ресурсам. Анализ и прогнозирование угроз можно проводить путем анализа существующей инфраструктуры.

Для этого можно использовать метод причинно-следственного анализа, который позволяет получить множества (совокупности) протекающих в инфраструктуре предприятия процессов и задать отношения подчиненности на этом множестве, отражающие реальную причинно-следственную структуру такого явления как обеспечение безопасности информации.

Проведя причинно-следственный анализ влияния различных факторов на уровень защищенности, с большой долей вероятности можно будет утверждать, что:

− некоторые угрозы могут быть реализованы только при определенных условиях;

− условия реализации угроз существуют и имеются косвенные факторы, влияющие на них;

− возможно, принимать решения, ведущие к скорейшему наступлению определенных благоприятных или ненаступлению неблагоприятных событий.

Фактически результатом начального проведения причинно-следственного анализа будет модель исходной защищенности информации предприятия.

Создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения ущерба включает в себя применения предыдущих двух пунктов для существующей инфраструктуры.

Один из самых, пожалуй, важных моментов, которые часто упускают из виду при проектировании и внедрении защищенной информационной инфраструктуры это конечно создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании. Этот пункт включает в себя комплекс мер и противодействий, таких как, например, анализирование входящего и исходящего трафика, анализирование изменения вносимых в системные файлы и пользовательские файлы, изменения, вносимые в служебную информацию, передаваемую от одного узла системы к другому узлу. К этому пункту так же можно отнести и анализирование новых тенденций, как в информационной безопасности, так и новых тенденций и направлений в процессах взлома систем и отдельных узлов систем.

Отдельным пунктом необходимо выделить пункт создание условий для максимально возможного возмещения и локализации ущерба, потому как систем, которые не могут быть взломаны и нарушены, не существует, и не учитывать этого мы не можем. От нас требуется определить критические ресурсы и критические данные, определить механизмы их восстановления при физическом сбое, злонамеренном действии третьих лиц или иных негативных процессах.

Цель и задачи исследования. Одним из важнейших направлений исследований в области информационной безопасности являются работы, связанные с изучением различных аспектов обеспечения безопасности компьютерных сетей и систем. В статье рассматриваются основные направления научных изысканий в области компьютерной безопасности.

Основные этапы построения защищенной инфраструктуры. На рис. 1 можно видеть блок-схему основных этапов построения защищенной информационной инфраструктуры.

Рис. 1 – Основные этапы построения защищенной инфраструктуры

Постановка задачи собственно сама идея, что мы будем защищать, сколько мы готовы потратить на защиту, сколько целесообразно потратить на защиту.

Сбор и анализ данных включает в себя анализ бизнес-процессов, какие порождают процессы они от кого они зависят и т. д.

Внедрение системы включает в себя выбор самой системы или комплекса систем, разработка правил и внедрение в пилотный проект этих систем и правил на предприятии.

Проверка работоспособности систем и правил, возможно, доработка систем под нужды бизнес-процессов и описание всех мер и правил, а также описание систем. Определение рисков и принятие рисков, и как противовес к пониманию рисков описание действий при чрезвычайных ситуациях и описание восполняемых и не восполняемых потерях.

Запуск всего комплекса мер подразумевает запуск в продакшен всей системы, проверка как работает эта система. Как одна из проверок работоспособности системы есть периодическая проверка, например, на проникновение, так называемый Penetration test. При работе системы обязательно будет анализироваться ее работа и как следствие будет появляться улучшения, что будет в свою очередь запускать по новой процесс улучшения информационной безопасности.

Представим более детальное описание блок схемы, а именно части схемы “Сбор и анализ данных”

Для построения эффективной и безопасной ИТ инфраструктуры необходимо понимать какие бизнес-процессы будут ее использовать и как. Для этого необходимо их описать.

Бизнес-процесс – это регулярно повторяющаяся последовательность взаимосвязанных мероприятий (операций, процедур, действий), при выполнении которых используются ресурсы внешней среды, создается ценность для потребителя и выдается ему результат.

Потребитель может быть как внешним, так и внутренним по отношению к организации. *Внешний потребитель* – это потребитель, который не входит в состав данной организации, а *внутренний* – тот потребитель, который находится в рамках данной организации.

Подробная классификация бизнес-процессов имеет следующий вид: основные процессы, сопутствующие процессы, вспомогательные процессы, обеспечивающие процессы, управляющие процессы, процессы развития.

Основными бизнес-процессами являются процессы, ориентированные на производство товара или оказание услуги, являющиеся целевыми объектами создания предприятия и обеспечивающие получение дохода.

Сопутствующие процессы – процессы, ориентированные на производство товара или оказание услуги, являющиеся результатами сопутствующей основному производству производственной деятельности и также обеспечивающие получение дохода.

Вспомогательные бизнес-процессы – процессы, предназначенные для обеспечения выполнения основных БП и поддержания их специфических черт.

Обеспечивающие бизнес-процессы – процессы, предназначенные для жизнеобеспечения всех остальных БП и ориентированные на поддержку их универсальных черт

Бизнес-процессы управления – это процессы, охватывающие весь комплекс функций управления на уровне каждого БП и бизнес-системы в целом. Это процессы стратегического, оперативного и текущего планирования, формирования и осуществления управленческих воздействий.

Бизнес-процессы развития – это процессы совершенствования производимого товара или услуги, технологий, модификации оборудования.

На рис 2. мы видим Схему описания процесса. Схематически ее можно разделить на 5 главных частей.

Рис. 2 – Схема описания процесса

Бизнес-процесс – устойчивая, целенаправленная совокупность взаимосвязанных видов деятельности (последовательность работ), которая по определенной технологии преобразует входы в выходы по определенным правилам с помощью определенных механизмов.

В качестве входа процесса может быть информация (документ), товарно-материальная ценность или сотрудник (обычно, это процессы отдела кадров). В качестве выхода процесса могут быть все те же элементы, что и на входе, но уже преобразованные в определенное состояние в результате выполнения процесса.

Управление процесса - как правило, информация, которая определяет правила преобразования входов в выход. Механизм процесса - то, что преобразует вход в выход. Механизмами, как правило, являются сотрудники (структурные подразделения) организации и техника, на которой они работают (станки, оргтехника).

В таб.1 мы можем видеть разделение информационной безопасности на два направления, причем они могут работать одна независимо от другой, но наибольшей эффективности они достигнут в синергии друг с другом, потому как будут дополнять друг друга

Таблица 1 – Направления информационной безопасности

Активная безопасность	**Пассивная безопасность**
• Антивирусная безопасность • Разграничение прав • Система сетевой безопасности • Система противодействия сетевым атакам • Система антиспам • Патч-менеджмент	• Система анализа сетевого трафика • Система анализа внутренней сетевой активности • Анализатор почты • Система анализа внесения изменений в критические процессы и узловые системы

К активной безопасности можно отнести такие типы безопасности как антивирусная безопасность, разграничение прав доступа, антиспам система и т.д., активной она называется так, потому что активно воздействует на все систему в целом.

Пассивная безопасность не менее важна, чем активная. Пассивной она называется, потому что она не воздействует на систему, а только собирает данные с нее и анализирует их.

К пассивной системе можно отнести такие системы как, например система анализа сетевого трафика, анализатор почты, система сбора лог-файлов, система анализа изменения, вносимые в конфигурации и критические процессы и узлы системы.

Детальнее разберем внедрение системы разграничения прав пользователей.

Этот процесс можно разбить на несколько процессов и представить в виде блок-схемы на рис. 3:

Рис. 3 – Внедрение системы разграничения прав доступа пользователей ИС

Первый блок будет “Определение ролей пользователей и объектов ИС”. Формирование ролей призвано определить чёткие и понятные для пользователей компьютерной системы правила разграничения доступа. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа.

Второй блок “Определение правил взаимодействия объектов и ролей”. Определим правила, по которым будут взаимодействовать роли с объектами системы. В третьем блоке анализируем взаимодействие объектов и ролей ИС между собой, как это будет проходить и что для этого взаимодействия еще необходимо. В четвертом блоке описываем и формализуем информацию, полученную в процессе внедрения системы разграничения прав на основе ролей. В последнем блоке непосредственно уже вносим изменения в саму ИС.

Подробнее остановимся на ролевой модели предоставления доступа.

При использовании ролевой политики управление доступом осуществляется в две стадии:

Во-первых, для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам.

Во-вторых, каждому пользователю назначается список доступных ему ролей.

Формирование ролей призвано определить чёткие и понятные правила разграничения доступа. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически правила разграничения доступа.

Несмотря на то, что Роль является совокупностью прав доступа, ролевое управление доступом отнюдь не является частным случаем избирательного управления доступом, так как его правила определяют порядок предоставления доступа субъектам компьютерной системы в зависимости от имеющихся (или отсутствующих) у него ролей в каждый момент времени.

Так как привилегии не назначаются пользователям непосредственно и приобретаются ими только через свою роль (или роли), управление индивидуальными правами пользователя, по сути, сводится к назначению ему ролей. Это упрощает такие операции, как добавление пользователя или смена подразделения пользователем.

Рассмотрим ролевую модель предоставления доступа, описанную на математическом языке, ролевую модель можно представить, как несколько множеств, а именно:

U-множество пользователей,

R- множество ролей,

P- множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа

S- множество сеансов работ пользователей с системой.

Как можно видеть PA-P×R отображает множество полномочий на множество ролей, устанавливая для каждой роли набор присвоенных ей полномочий. UA-U×R отображает множество пользователей на множество ролей, определяя для каждого пользователя набор доступных ему ролей.

Множество назначений пользователей есть подмножество субъектов и ролей. Правила управления доступом ролевой политики безопасности определяются следующими функциями:

user:S→U - для каждого сеанса S эта функция определяет пользователя, который осуществляет этот сеанс работы с системой.

user(s) = uroles:S→P(R) - для каждого сеанса S эта функция определяет набор ролей из множества R

которые могут быть одновременно доступны пользователю в этом сеансе.

roles(s)={ri| (user(s), ri) ∈UA};

permissions: S→P - для каждого сеанса S эта функция задает набор доступных в нем полномочии, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе: permissions(s) = Ur∈roles(s){Pi, (Pi, r)∈PA).

Математическая модель, описывающая поведение системы в условиях воздействия злоумышленного ПО. Разберем более детально, как может себя повести система при вирусном заражении. Возьмем за пример модель Прогрессивную (Подозрительный-зараженный-обнаруженный-вылеченный-топология) или сокращенно PSIDRT. Всю систему мы можем описать как сумму количества уязвимых, зараженных и вылеченных объектов.

Мы выделяем 2 этапа:

1) Только заражение объектов (модель идентична модели *SI*)

2) Добавление фактора лечения, при этом вылеченные узлы не заражаются повторно.

Обобщенная структура компьютерной системы может быть представлена с помощью выражения:

$$N = S(t) + I(t) + D(t) + R(t),$$

где N – общее количество объектов в системе; $S(t)$ – количество уязвимых объектов; $I(t)$ – количество зараженных объектов; $R(t)$ –количество вылеченных объектов, обладающие иммунитетом; $D(t)$ – количество объектов, в которых обнаружен вирус.

Модель характеризуется наличием четырех типов объектов управления: зараженные (I), не зараженные (S), вылеченные объекты, обладающие иммунитетом (R), и количество объектов, в которых обнаружен вирус (D).

Выводы

1. Нами были рассмотрены только основные три составляющие информационной безопасности, внедрение которых в совокупности может решить около 80 % всех проблем информационной безопасности.

2. В вопросе построения устойчивой и безопасной ИТ-инфраструктуры необходимо находить баланс между защищенностью и бизнес-ориентацией ИТ-инфраструктуры, так как чем сложнее система информационной безопасности, тем сложнее пользователю бизнес-процессов ее использовать и как следствие падает КПД бизнес-процессов.

Список литературы:

1. *Котенко, И. В.* Перспективные направления исследований в области компьютерной безопасности [Текст] / *И. В. Котенко, Р. М. Юсупов* //Защита информации. Инсайд. – 2006. – Т. 2, №. 6. – С. 46–57.
2. *Чипига, А. Ф.* Оценка эффективности защищённости автоматизированных систем от несанкционированного доступа [Текст] / *А. Ф. Чипига, В. С. Пелешенко* // Вестник СевКавГТУ. Серия «Физико-химическая». – 2004. – №1 (8). – С. 40.
3. *Мещеряков, Р. В.* Основы информационной безопасности [Текст] / *Р. В. Мещеряков, А. А. Шелупанов, Е. Б. Белов, В. П. Лось*. – М.: Горячая линия–Телеком, 2006. – 544 с.
4. *Шварцман, В. О.* Количественная оценка защищенности информации и сетей святи от несанкционированных действий [Текст] / *В. О. Шварцман, // В. О. Шварц* / Электросвязь. – 2008. – № 5. – С. 5–8.
5. *Нечунаев В. М.* Методика описания корпоративной информационной системы для процедуры управления рисками информационной безопасности [Текст] // *В. М. Нечуев* / Доклады ТУСУРа. – 2008. – № 2 (18). – С. 116–117.
6. *Домарев, В. В.* Безопасность информационных технологий. Методология создания систем защиты [Текст] / *В. В. Домарев*. – Киев: ТИД ДиаСофт, 2002. – 688 с.
7. *Давыдов, И. В.* Формализация модели совершения киберпреступлений, совершаемых с использованием вредоносных кодов [Текст] / *И. В. Давыдов, А. А. Шелупанов* // Известия Томского политехнического университета. – 2006. – Т. 309, № 8. – *С. 126–129*.
8. *Репин, В. В.* Процессный подход к управлению. Моделирование бизнес-процессов [Текст] / *В. В. Репин, И. В. Елиферов*. – «Манн, Иванов и Фербер», 2012. – 544 с.
9. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа [Текст] / *А. Ю. Щеглов.* – Наука и Техника, 2004. – 384 с.
10. *Вентцель, Е. С.* Прикладные задачи теорий вероятностей [Текст] / *Е. С. Вентцель, Л. А. Овчаров*. – Москва: Академия, 2003.– 448 с.

References

1. Kotenko, Y. V. (2006). Prospective areas of research in the field of computer security. Data protection. Inside, 2 (6), 46–57.
2. Chypygha, A. F. (2004). Evaluation of the effectiveness of the protection of automated systems from unauthorized access. Vestnyk SevKavGhTU. Seryja «Fyzyko-khymycheskaja», 1 (8), 40.
3. Meshcheryakov, R. V., Shelupanov, A. A, Belov, E. B., Los, V. P. (2006). Fundamentals of Information Security. Moscow: Hot line-Telecom, 544.
4. Shvartsman, V. O. (2008). Quantitative assessment of information security and holy networks from unauthorized actions. Electrosvyaz, 5, 5–8.
5. Nechunayev, V. M. (2008). Method of describing the corporate information system for the information security risk management procedure. Reports of TUSUR, 2 (18), 116–117.
6. Domarev, V. V. (2001). The security of information technology. Methodology of creating protection systems. Kiev: TID DiaSoft, 688.
7. Davydov, I. V., Shelupanov, A. A. (2006). Formalization of the model of committing cybercrime committed with the use of malicious codes. Bulletin of the Tomsk Polytechnic University, 309 (8), 126–129.
8. Repin, V. V., Eliferov, V. G. (2012). Process approach to management. Modeling of business processes. «Mann, Ivanov i Ferber», 544.
9. Shcheglov, A. Y. (2004). Protection of computer information from unauthorized access. Science and Technology, 383.
10. Venttsel, E. S., Ovcharov, L. A. (2003). Applied Problems of Probability Theory. Moscow: Academy, 448.

Поступила (received) 11.11.2016

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Побудова безпечної інформаційної інфраструктури як необхідність виживання/ О. Г. Оксіюк, Я. В. Шестак, Д. О. Огбу// Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2016. – No 50(1222). – С.112–117. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Построение безопасной информационной инфраструктуры как необходимость выживания/ А. Г. Оксиюк, Я. В. Шестак, Д. О. Огбу// Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2016. – No 50(1222). – С.112–117. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Building a secure information infrastructure as a necessity for survival/ A. G. Oksiuk, Y.V. Shestak, J. O. Ogbu//Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2016. – No 50 (1222).– P. 112–117. – Bibliogr.: 10. – ISSN 2079-5459.

Відомості про авторів / Сведения об авторах / About the Authors

Оксіюк Олександр Глібович - доктор технічних наук, Київський національний університет імені Тараса Шевченка, професор, завідувач кафедри «Кібербезпеки та захисту інформації»; вул. Володимирська, 60, м. Київ, Україна, 01033; e-mail: o.oksiuk@gmail.com.

Шестак Яніна Володимирівна - аспірант, Київський національний університет імені Тараса Шевченка, кафедра «Кібербезпеки та захисту інформації»; вул. Володимирська, 60, м. Київ, Україна, 01033; e-mail: lucenko.y@ukr.net.

Огбу Джеймс Онигван – аспірант, Київський національний університет імені Тараса Шевченка, кафедра «Кібербезпеки та захисту інформації»; вул. Володимирська, 60, м. Київ, Україна, 01033; e-mail: jamesybone@yahoo.com.

Оксиюк Александр Глебович - доктор технических наук, Киевский национальный университет имени Тараса Шевченко, профессор, заведующий кафедрой «Кибербезопасности и защиты информации»; ул. Владимирская, 60, г. Киев, Украина, 01033; e-mail: o.oksiuk@gmail.com.

Шестак Янина Владимировна - аспирант, Киевский национальный университет имени Тараса Шевченко, кафедра «Кибербезопасности и защиты информации»; ул. Владимирская, 60, г. Киев, Украина, 01033.

Огбу Джеймс Онигван - аспирант, Киевский национальный университет имени Тараса Шевченко, кафедра «Кибербезопасности и защиты информации»; ул. Владимирская, 60, г. Киев, Украина, 01033; e-mail: jamesybone@yahoo.com.

Oksiuk Alexandr Glebovich - doctor of technical science, Taras Shevchenko National University of Kyiv, professor, head of «Cyber security and information protection»; Volodymyrska str., 60, City of Kyiv, Ukraine, 01033.

Shestak Yanina Vladimirovna - PG student, Taras Shevchenko National University of Kyiv, department «Cyber security and information protection»; Volodymyrska str., 60, City of Kyiv, Ukraine, 01033; e-mail: lucenko.y@ukr.net.

James Ogbu - PG student, Taras Shevchenko National University of Kyiv, department «Cyber security and information protection»; Volodymyrska str., 60, City of Kyiv, Ukraine, 01033; e-mail: jamesybone@yahoo.com.

УДК 621.74

Ю. В. ОРЕНДАРЧУК, А. А. КРАСНОУХОВА, І. О. АЧКАСОВ, А. С. БАРСУК, В. І. ГОЛОВКО

ОПТИМІЗАЦІЯ СКЛАДУ ФОРМУВАЛЬНИХ СУМІШЕЙ ДЛЯ АВТОМАТИЗОВАНОГО ВИРОБНИЦТВА ЛИТИХ ДЕТАЛЕЙ ДВИГУНІВ ВНУТРІШНЬОГО ЗГОРЯННЯ

На основі гребеневого аналізу вирішена оптимізаційна задача щодо визначення параметрів формувальної суміші типу холоднотвердіючої суміші (ХТС). В якості критеріїв оптимізації обрано максимум живучості та мінімум осипає мості суміші. Вхідними змінними обрано вміст у суміші рідкого скла та пропілен карбонату. Показано, що теоретично можна досягти максимального значення живучості 15,5 хв і мінімального значення осипаємості 0,04 %. Отримані результати можуть бути використані в автоматизованому виробництві формувальної суміші для підвищення якості литих деталей ДВЗ.

Ключові слова: двигуни внутрішнього згоряння, формувальна суміш, холоднотвердіючої суміш, гребеневий аналіз

На основе комбинированный анализа решена оптимизационная задача по определению параметров формовочной смеси типа холоднотвердеющих смеси (ХТС). В качестве критериев оптимизации выбрана максимум живучести и минимум осыпает мосту смеси. Входными переменными избран содержание в смеси жидкого стекла и пропилен карбоната. Показано, что теоретически можно достичь максимального значения живучести 15,5 мин и минимального значения осипаемости 0,04%. Полученные результаты могут быть использованы в автоматизированном производстве формовочной смеси для повышения качества литых деталей ДВС.

Ключевые слова: двигатели внутреннего сгорания, формовочная смесь, холоднотвердеющих смесь, комбинированный анализ

On the basis of the combined analysis, an optimization problem is solved to determine the parameters of a molding mixture of the cold-hardening mixture (CHM) type. As a criterion of optimization, the maximum of survivability and the minimum of the mixture shedding are chosen. The contents of liquid glass and propylene carbonate in the mixture are chosen as input variables.

It is shown that the maximum of the survivability of the mixture is achieved with the limitations imposed by the experimental design is about 15.3 min. But if remove the restrictions, then theoretically it can reach of 15.5 minutes.

The minimum of the mixture shedding, when there are limitations imposed by the experimental design, corresponds to about 0.05. But, if remove the restrictions, it can reach of a minimum about 0.04%.

The obtained results can be used in the automated production of molding mixture to improve the quality of cast parts of ICE.

Keywords: internal combustion engines, molding mixture, cold-hardening mixture, combined analysis