УДК 629.039.58: 004.056.53

А.В. Дагаев, Ю.М. Бородянский, В.Б. Лебедев, А.В. Проскуряков, А.А. Ивахненко

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ЭНЕРГОГЕНЕРИРУЮЩИХ КОМПАНИЙ

Представлены основные понятия информационной безопасности, приведен спектр решаемых проблем, разработана классификация информационных ресурсов предприятия, угроз и уязвимостей в программно-аппаратном сетевом комплексе, показаны недостатки в защите корпоративной информационной сети.

Анализ; безопасность; сеть.

A. V. Dagaev, U. M. Borodyansky, V.B. Lebedev, A. V. Proskuryakov, A.A. Ivahnenko

THE ANALYSIS OF SECURITY IN COMPUTER NETWORKS OF THE POWER GENERATING COMPANIES

This article focuses on the basic concepts of information security; a range of current problems; the classification of the corporate information resources; risks and vulnerabilities in the hardware-software network complex; imperfections in the corporate network shield

Stock; system.

Развитие информационных технологий в последние десятилетия приводит к развитию теории информационной надежности и безопасности хранения информации. Это связано также с тем, что растут объемы информации, хранимой в электронном виде, и увеличивается ее разнообразие, выдвигаются новые требования к методам доступа и передачи информации, качественно изменяются средства хранения, резервирования и обработки информации. Анализ характеристик защиты информационных систем и мероприятий, направленных на ее повышение, позволяет выяснить плохо защищенные места системы, условия, при которых может быть нарушена защита и реализован несанкционированный доступ к информации, дает возможность формализовать и выработать оптимальную последовательность действий, приводящую к более надежному и стабильному состоянию системы.

Под **информационной безопасностью** понимается комплекс мероприятий и средств по обеспечению сохранности информации, вводимой в информационную систему, передаваемой, обрабатываемой, хранимой или выдаваемой после обработки её средствами.

Уязвимость (Vulnerability) - представляет собой слабость в системе защиты, которая делает возможным реализацию угрозы.

Угроза (Threat) – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации. Потенциальная возможность получения несанкционированного доступа (НСД), которая обусловлена архитектурными особенностями используемых аппаратных и программных средств, используемых технологий, а также организацией работы с данными [1].

Анализ рисков – процесс определения угроз, уязвимостей, возможного ущерба,

а также контрмер.

Спектр проблем, решаемых в области информационной безопасности

Весь перечень проблем, возникающих при эксплуатации компьютерной техники и PC (рабочих станциях), можно представить в виде пирамиды, изображенной на рис. 1.

На нижнем уровне представлены локальные проблемы, решаемые на уровне PC. Эти проблемы могут иметь характер некорректной работы программного обеспечения, поломок оборудования, неправильных действий сотрудников и др.

Далее решаются проблемы, связанные с сетевым оборудованием и сетевой безопасностью PC. На этом уровне решаются проблемы несанкционированного доступа, поломок сетевого оборудования, потери доступа к сети.

На следующем уровне представлены проблемы, связанные с серверами. Это может быть поломка серверов, неправильная настройка серверных служб и приложений, ошибки в защите ОС и т.д.

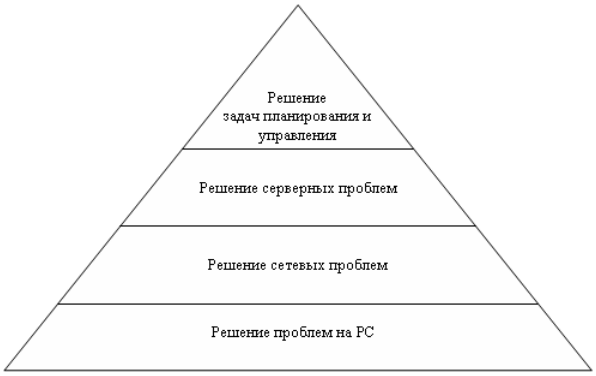

Рис. 1. Спектр проблем ИБ, возникающих при эксплуатации компьютерной техники

На самом верхнем уровне решаются задачи, связанные с утверждением перечня проводимых работ, принятием решения о внедрении новых технологий, выделением средств на закупку оборудования, постановкой задач перед сотрудниками и др.

Все проблемы, приведенные на рис.1, являются важными для информационной безопасности.

Описание ресурсов, уязвимостей и угроз

Управление рисками, рассмотренное в [2], является довольно трудоемкой проблемой. Оно состоит из рассмотрения ресурсов, используемых в сетях предприятия, уязвимостей, угроз. Рассмотрим вначале информационные ресурсы, все они имеют ряд уязвимостей (рис. 2). Ресурсы представляют собой совокупность средств, используемых для работы в корпоративной сети предприятия. Информационные ресурсы можно условно разбить на ресурсы программного, аппаратного обеспечения и ресурсы, состоящие из сотрудников предприятия.

Представленные ресурсы определяют перечень уязвимостей, которые могут быть в них выявлены. Методика определения ресурсов, изучения уязвимостей и устранения уязвимостей, а также угроз является основным компонентом в теории информационной безопасности. Самыми простыми для изучения из представленных выше компонентов риска, несомненно, являются ресурсы информационного центра предприятия.

Перечень ресурсов, используемых ИТ на предприятии, определяется выбором решаемых задач, количеством и структурой информации, находящейся в компонентах информационного центра, в том числе формализованными знаниями сотрудников предприятия, планами развития информационного центра, выделяемыми для развития информационного центра ресурсами разработки.

Первым компонентом ресурсов, представленным на рис.2, является программное обеспечение информационного центра. Оно состоит из следующих компонентов: сервисов ОС, локальных и сетевых паролей, файловой системы, протоколов передачи данных, антивирусного ПО, программ, установленных на РС и серверах, ПО для хранения пользовательских данных на РС и серверах, а также ПО для управления этими данными. По статистическим данным, самым уязвимым ресурсом ПО, с точки зрения реализации угрозы, является антивирусный пакет. Это связано с тем, что вероятность потери информации от вирусного воздействия очень большая.

Вторым компонентом ресурсов предприятия для ИТ является штат сотрудников, он разбивается на категории: персонал с низким уровнем знаний в области ИТ; персонал с доступом к ценной информации; квалифицированный персонал, сознательно наносящий ущерб. Самым уязвимым ресурсом в данном случае является персонал с низким уровнем знаний в области информационных технологий, поскольку отсутствие определенных навыков и знаний делает работу такого персонала на РС опасным как для себя, так и для других сотрудников. В данном случае на этом ресурсе могут реализоваться угрозы вирусной деятельности и случайной потери информации.

Аппаратное обеспечение является инструментом, позволяющим работать сотрудникам с информацией. Оно состоит из линий передачи данных, аппаратного обеспечения компьютеров, сетевого оборудования и средств хранения информации. Самыми ненадежными ресурсами аппаратного обеспечения являются жесткие диски.

По статистике именно они чаще всего выходят из строя, иногда нанося непоправимый ущерб организации. Поэтому использование технологии резервирования является необходимым условием уменьшения вероятности потери информации в случае поломки жесткого диска, как сервера, так и обычного РС.

Далее опишем уязвимости и угрозы, которые существуют для программно-аппаратного сетевого комплекса. Посредством использования уязвимостей ресурсов могут реализоваться угрозы. Уязвимости являются первой причиной потери информации в КИС, второй причиной являются угрозы.

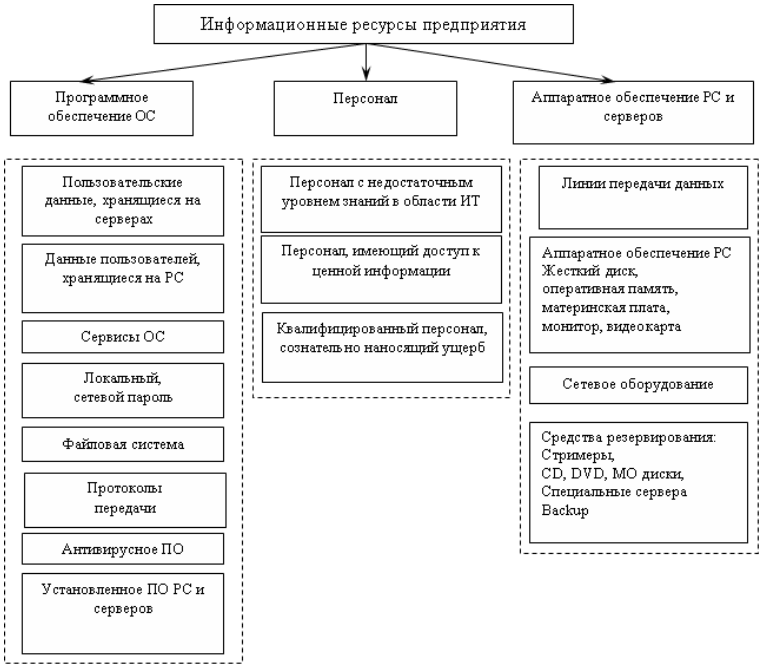

Рис.2. Перечень информационных ресурсов предприятия

Как и ресурсы уязвимости разбиваются на три типа - уязвимости со стороны ПО, уязвимости со стороны аппаратного обеспечения и уязвимости со стороны сотрудников, что представлено на рис. 3.

Исследование уязвимостей является одним из основных вопросов, которые приходится решать при обеспечении информационной безопасности информационного центра. Перечень уязвимостей отображает состояние защищенности информационных ресурсов, которые присутствуют в корпоративной информационной сети предприятия [4].

Наличие уязвимостей определяется: качеством программного обеспечения; типом ОС, которые установлены; частотой обновления ОС и ПО; уровнем знаний сотрудников в области информационных технологий и безопасности; надежностью аппаратного обеспечения; количеством РС; уровнем понимания проблем ИС и методами, используемыми при внедрении информационных систем. Комплексный показатель уязвимости определяет перечень угроз, которые могут реализоваться.

Уязвимости со стороны программного обеспечения состоят из уязвимостей: в защите ОС, незащищенных сервисов, недокументированных закладок ПО, ошибочной реализации функций работы с ОС установленных приложений, уязвимости паролей, файловой системы, протоколов передачи данных, антивирусного ПО, нелицензированного ПО, системных сервисов, отсутствия обновлений ОС.

По предварительным данным, самыми важными уязвимостями с точки зрения количества реализуемых на них угроз, являются отсутствие антивирусной защиты и использование нелицензированного ПО. Программные уязвимости представляются самыми многочисленными по сравнению с другими типами уязвимостей, что связано с их разнообразием.

Уязвимости со стороны сотрудников состоят из ряда уязвимостей: неза-

блокированного РС, пароля на рабочем месте, отсутствия системы резервирования информации, неправильных настроек ОС, уровня грамотности сотрудников в области программных средств, установленных на РС, уровнем корпоративной культуры групповой работы с информационными ресурсами, уязвимости, связанной с лояльностью персонала. Кроме того, отсутствие желания делиться открытой производственной информацией и работать сообща с другими участниками производственного процесса существенно снижает эффективность работы всего коллектива предприятия, отрицательно сказывается на конкурентоспособности выпускаемой продукции. На втором месте стоит отсутствие своевременного резервирования информации, далее – неправильные действия сотрудников при работе с программным обеспечением.

Уязвимость аппаратного обеспечения легче всего поддается формализации и классификации. Уязвимость со стороны аппаратного обеспечения разбивается на следующие категории: уязвимость неопломбированного РС, уязвимость ненадежных и старых носителей информации, уязвимость от ненадежной среды и средств передачи информации, уязвимость от неправильного функционирования средств передачи информации. Как показывает практика, самой важной уязвимостью представляется уязвимость старых и ненадежных носителей информации.

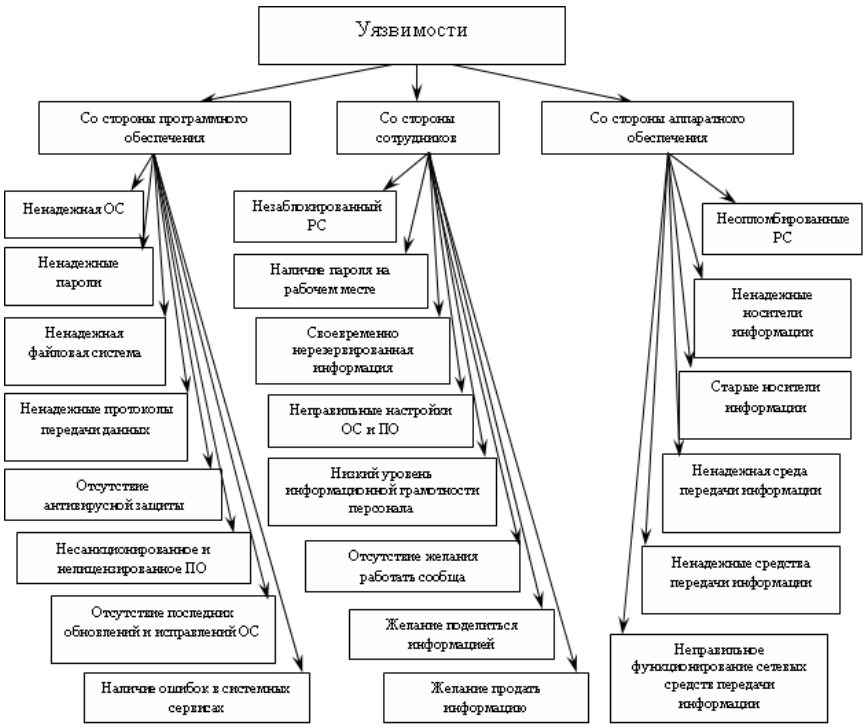

Рис. 3. Классификация уязвимостей корпоративной сети

Классификация угроз и уязвимостей проводится нами по объектам воздействия на ресурсы. В литературе встречаются другие типы классификации, так, например, в [3] представлена классификация угроз по способу их осуществления.

Следует отметить, что ресурсы, уязвимости и угрозы состоят из трех ос-

новных компонент – аппаратной, программной и компоненты сотрудников. Это обусловлено спецификой компьютерной техники и наличием программного обеспечения, которое создает интерфейсный уровень взаимодействия сотрудника и аппаратного обеспечения. Далее рассмотрим угрозы, которые могут существовать в программно-аппаратного сетевом комплексе. (рис.4.)

Угрозы от сотрудников представляют самый широкий набор угроз, вследствие многообразий действий сотрудников по отношению к программному и аппаратному обеспечению. Однако заметим, что мощность угроз со стороны сотрудников сравнима с мощностью угроз со стороны программного обеспечения. Не будем описывать весь спектр угроз, которые может реализовывать персонал предприятия, отметим только, что они разбиваются на прямые, случайные и косвенные. Прямые угрозы это угрозы осознанного действия злоумышленника по отношению к аппаратуре и информации, которая передается по сети или хранится на носителях. Также возможен случай разглашения информации. К случайным угрозам относится случайный доступ к конфиденциальной информации, который может быть обусловлен ошибками функционирования ПО, неправильными настройками сети и ОС, непреднамеренными действиями, которые привели к несанкционированному доступу и др.

Косвенные угрозы определяются получением конфиденциальной информации посредством проведения дополнительного анализа имеющихся данных, посредством использования отработанных средств хранения информации. Самыми опасными угрозами данного типа являются: неправильная работа с ПО и нежелание делиться информацией.

Уязвимости и вероятные угрозы

Угрозы со стороны программного обеспечения чаще всего реализуются на антивирусной уязвимости и уязвимости основных сервисов ОС. Программных угроз гораздо меньше, чем уязвимостей. Они представлены тремя компонентами: использование несанкционированного ПО, утрата информации от неправильной работы ПО и разрушение информации при воздействии вирусов. Следует отметить, что в большинстве случаев самым незащищенным ресурсам соответствуют самые важные уязвимости и опасные угрозы, это происходит вследствие того, что на уязвимостях таких ресурсов реализация угроз наиболее вероятна.

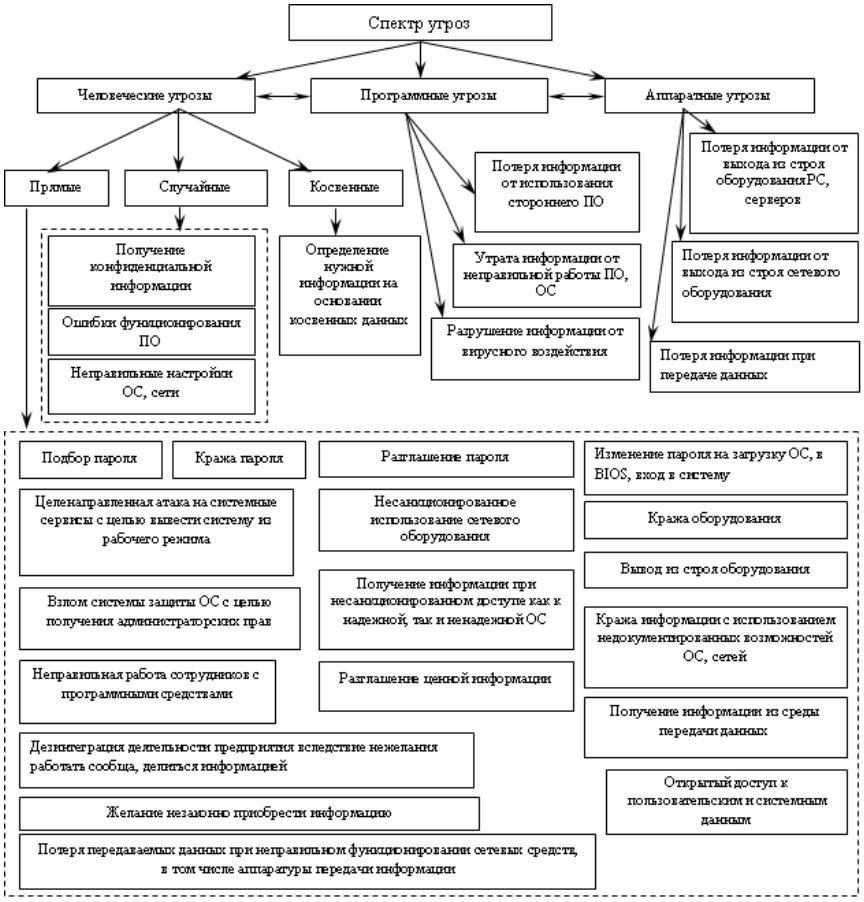

Рис.4. Угрозы корпоративной сети

Уязвимости отражают факт отказа оборудования. Таким образом, информация может быть потеряна при передаче данных по сети, при работе накопителей, хранящих информацию, и при выходе из строя сетевого оборудования.

У каждого ресурса, представленного на рис. 2, имеется ряд уязвимостей, каждой уязвимости соответствует перечень угроз.

В табл.1 представлены наиболее вероятные, по нашему мнению угрозы, которые могут реализоваться на соответствующих уязвимостях.

Для более детального рассмотрения уязвимостей и соответствующих им угроз надо составлять таблицы их соответствия и проводить обработку экспертных данных с применением аппарата теории вероятностей, теории статистики и теории надежности.

В табл.2 представлен перечень ресурсов и соответствующие им важные угрозы.

Таблица 1

Уязвимости и вероятные угрозы

Уязвимость	Наиболее вероятная угроза, которая может реализоваться на данной уязвимости
Со стороны программного обеспечения	
Ненадежная ОС (комплексный показатель)	Прямой доступ к ненадежной ОС
Ненадежные пароли	Подбор пароля
Ненадежная файловая система	Получение информации при несанкционированном доступе к ненадежной ОС
Ненадежные протоколы передачи данных	Получение информации из среды передачи данных
Отсутствие последних обновлений и исправлений ОС	Использование недокументированных возможностей ОС
Отсутствие антивирусной защиты	Разрушение информации от вирусного воздействия
Несанкционированное и нелицензированное ПО	Потеря информации от использования стороннего ПО
Наличие ошибок в системных сервисах	Несанкционированный доступ к пользовательским и системным данным
Со стороны сотрудников	
Незаблокированный РС	Получение информации при несанкционированном доступе к ОС
Наличие пароля на рабочем месте	Кража пароля
Ненадежные пароли	Подбор пароля
Своевременно нерезервированная информация	Потеря информации от выхода из строя оборудования
Неправильные настройки ОС и ПО	Кража информации с использованием недокументированные возможности ОС
Низкий уровень информационной грамотности персонала	Потеря информации при неправильной работа сотрудников с программными средствами
Отсутствие желания работать сообща	Дезинтеграция деятельности предприятия
Со стороны аппаратного обеспечения	
Неопломбированные РС	Изменение пароля на вход в систему, в BIOS
Ненадежные компоненты РС	Потеря информации от выхода из строя оборудования
Старые компоненты РС	Потеря информации от выхода из строя оборудования
Ненадежная среда передачи информации	Хищение информации с использованием недокументированных возможностей сетей
Ненадежные средства передачи информации	Потеря информации при передаче данных

Для каждой уязвимости приведена угроза, реализация которой наиболее вероятна. Экспертное оценивание можно также провести по имеющимся ресурсам и соответствующим им угрозам. Эта процедура осуществляется для выяснения того, какая угроза самая опасная для данного ресурса. После проведения опроса, в котором угрозы ранжируются по степени важности для каждого ресурса, сведения усредняются по всем экспертам. Далее рассматриваются самые важные ресурсы для предприятия и самые опасные угрозы, которые могут на них реализоваться. На следующем этапе проводятся мероприятия по устранению уязвимостей и уменьшению влияния угроз [5].

Таблица 2

Ресурсы и уязвимости

Важность ресурса	Название ресурса	Наиболее важная уязвимость	Реализация наиболее вероятной угрозы
1	Пользовательские данные на PC	Наличие пароля на рабочем месте	Кража пароля
2	Антивирусное ПО	Отсутствие антивирусной защиты	Разрушение информации от вирусного воздействия
3	Пользовательские данные на серверах	Отсутствие последних обновлений и исправлений ОС	Использование недокументированных возможностей ОС
4	Персонал с низким уровнем знаний в области ИТ	Низкий уровень информационной грамотности персонала	Потеря информации при неправильной работа сотрудников с программными средствами
5	Локальный, сетевой пароль	Ненадежные пароли	Подбор пароля
6	ПО на PC и серверах	Низкий уровень информационной грамотности персонала	Потеря информации при неправильной работе сотрудников с программными средствами
7	Средства резервирования	Своевременно нерезервированная информация	Потеря информации от выхода из строя оборудования
8	Персонал, владеющий кофиденциальной информацией	Нарушение мер по соблюдению конфиденциальности	Разглашение конфиденциальной информации
9	Сервисы ОС	Наличие ошибок в системных сервисах	Несанкционированный доступ к пользовательским и системным данным
10	Файловая система	Ненадежная файловая система	Получение информации при несанкционированном доступе к ненадежной ОС
11	Протоколы передачи	Ненадежные протоколы передачи данных	Получение информации из среды передачи данных
12	Аппаратное обеспечение PC	Ненадежные компоненты PC	Потеря информации от выхода из строя оборудования
13	Линии передачи данных	Ненадежные средства передачи информации	Потеря информации при передаче данных
14	Сетевое оборудование	Неправильное функционирование сетевых средств передачи информации	Потеря передаваемых данных при неправильном функционировании сетевых средств передачи данных
15	Квалифицированный персонал, сознательно наносящий ущерб	Преступность в сфере информационных технологий	Незаконное приобретение сторонними лицами конфиденциальной информации

Заключение. Информационная безопасность играет все большую роль в жизни любого предприятия. Особенно это касается предприятий работающих в условиях жесткой конкуренции. Рассмотренная классификация уязвимостей и угроз позволяет показать «узкие» места в информационной безопасности в корпоративной сети, что позволит принять меры по её улучшению и снизить риск возможности несанкционированного доступа к ценной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах «Дмк». – М., 2002. – 656с.
2. *Афанасьев А.* Безопасность корпоративной сети: защита изнутри. Журнал Intelligent enterprise (Корпоративные системы), СК Пресс №24(89), www.iemag.ru. – Москва, 23 декабря 2003г. – 48с.
3. *Конеев И., Беляев А.* Информационная безопасность предприятия. – СПб.: “БХВ-Петербург”, 2003. – 733с.
4. *Галактионов В.* Системная архитектура и ее место в архитектуре предпри-

ятия. ДИС. – № 5, 2002. – С. 6-16.
5. *Астахов А.* Разработка эффективных политик информационной безопасности // IT Директор – №1. – 2005.

Дагаев Александр Владимирович
Технологический институт федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге
E-mail: fin_val_iv@tsure.ru
347928, Таганрог, ГСП 17А, Некрасовский, 44. Тел: 88634-371-689

Лебедев Владимир Борисович
E-mail: fin_val_iv@tsure.ru
Тел: 88634-311-310

Бородянский Юрий Михайлович
E-mail: fin_val_iv@tsure.ru
Тел: 88634-311-310

Ивахненко Александр Александрович
E-mail: fin_val_iv@tsure.ru
Тел: 88634-311-310

Проскуриков Александр Викторови
E-mail: fin_val_iv@tsure.ru
Тел: 88634-311-310

Dagaev Alexandr Vladimirovich
Taganrog Institute of Technology - Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University
E-mail: fin_val_iv@tsure.ru
44, Nekrasovsky, Taganrog, 347928. Phone: 88634-371-689

Lebedev Vladimir Borisovich
E-mail: fin_val_iv@tsure.ru
Phone: 88634-311-310

Borodiansky Ury Mikhailovich
E-mail: fin_val_iv@tsure.ru
Phone: 88634-311-310

Ikhvanenko Alexandr Alexandrovich
E-mail: fin_val_iv@tsure.ru
Phone: 88634-311-310

УДК 681.3.06

Н.В. Драгныш

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ И МОДЕЛЕЙ ПОСТРОЕНИЯ КОМПЛЕКСОВ ПРОГРАММ

Рассмотрены базовые модели и принципы построения комплексов программ, основанные на разработках в процессе проектирования, анализа и син-