DOI 10.37882/2223–2966.2022.11.24

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ АВТОМАТИЗАЦИИ СОВРЕМЕННЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

STUDY OF THE PECULIARITIES OF ENSURING INFORMATION PROTECTION IN THE PROCESS OF AUTOMATION OF MODERN MEDICAL INSTITUTIONS

N. Moskvina

Summary. The main direction in the development of information technology is to ensure the information security of computer systems and software and hardware. In modern conditions, information is the basic basis in the process of activity of both an individual and society as a whole. Along with the development of science, there is an inevitable complication of the information model of the world. The quality of life of mankind directly depends on the degree of understanding of the flow of information processes.

This article is devoted to the study of the features of ensuring the protection of information in the process of automation of modern medical institutions. The article analyzes the features of automating the activities of modern medical institutions, the features of ensuring the protection of information in the process of automation, and explores typical information resources that participate in the information exchange of medical institutions.

Keywords: automation, medical institutions, information security, information resources, medical data, information protection, automated information systems.

Москвина Надежда Андреевна
Аспирант
Российский экономический университет имени Г.В. Плеханова, Москва
cheshirewhitecat@yandex.ru

Аннотация. Основное направление развития информационных технологий — обеспечение информационной безопасности компьютерных систем и программно-аппаратных средств. В современных условиях информация является базовой основой в процессе деятельности как отдельного человека, так и общества в целом. Вместе с развитием науки происходит неизбежное усложнение информационной модели мира. Качество жизни человечества напрямую зависит от степени понимания протекания информационных процессов.

Настоящая статья посвящена исследованию особенностей обеспечения защиты информации в процессе автоматизации современных медицинских учреждений. В статье произведен анализ особенностей автоматизации деятельности современных медицинских учреждений, особенностей обеспечения защиты информации в процессе автоматизации, исследованы типовые информационные ресурсы, которые участвуют в информационном обмене медицинских учреждений.

Ключевые слова: автоматизация, медицинские учреждения, информационная безопасность, информационные ресурсы, медицинские данные, защита информации, автоматизированные информационные системы.

Введение

Тема настоящей статьи — «Исследование особенностей обеспечения защиты информации в процессе автоматизации современных медицинских учреждений».

Актуальность выбранной темы можно объяснить тем, что в настоящее время наметилась тенденция постоянного роста числа потенциальных угроз конфиденциальности информации при обработке в автоматизированных системах в том числе и в медицинской сфере. Этот рост объясняется совершенствованием технических средств, компьютеризацией страны, возможностью всестороннего доступа к базам данных [1].

Цель статьи — исследование уязвимостей информационных ресурсов медицинских организаций при

их обработке в автоматизированных информационных системах и разработка модели угроз и модели нарушителя при автоматизированной обработке.

Объект исследования — система защиты информации в автоматизированных информационных системах медицинских учреждениях.

Предмет исследования — обеспечение информационной безопасности автоматизированных информационных системах медицинских учреждениях.

В процессе выполнения статьи использованы следующие общенаучные методы познания: анализ, синтез, дедукция, индукция.

Основная часть

Нынешние масштабы использования программно-аппаратных средств в медицинской сфере предрасполагают к появлению угроз, связанных с возможностью потери, искажения, данных, которые адресованы или принадлежат владельцам информации. В процессе анализа уязвимостей объекта защиты используется ряд критериев оценки. Наиболее распространенными и применяемыми критериями являются: степень защищенности информационных ресурсов, количество используемых процедур в процессе защиты информации, степень совместимости применяемых процедур, объем капитальных вложений на организацию системы защиты информации [2]. Для проверки достоверности и эффективности системы защиты информационных ресурсов медицинских учреждений применяются различные виды данных, отражающих работу защитной системы. Также для этих целей применяются различные отчетные документы и данные о результатах проводимой работы. Основные задачи проведения оценки степени защиты информационных ресурсов рассматриваются в контексте конкретного медицинского объекта, а также его роли в системе. Область проведенной оценки определяется применяемой моделью. В этой модели отражены основные параметры проводимого анализа безопасности баз данных. Основными критериями эффективности аудита информационной безопасности являются [3]:

- оценка рисков на организационном уровне;
- снижения рисков;
- повторные оценки рисков;
- оценка рисков на техническом уровне;
- учет рисков, связанных с использованием технологий.

Неотъемлемой частью упреждающей методики является анализ информации центров изучения проблем информационной безопасности. Работы по исследованию уровня безопасности информационных ресурсов проводятся в соответствии с требованиями международного стандарта ISO 17799. В состав этого стандарта входят основные требования к процедуре проверки эффективности информационной безопасности организаций. Также этот документ предусматривает определенную форму. В соответствии с этой формой осуществляется оформление результатов проверок. Отчет должен содержать информацию о всех выявленных потенциальных опасностях для баз данных медицинских организаций [4].

В большинстве случаев, медицинские организации нуждаются в систематическом проведении оценки уязвимости информационной безопасности при обработке данных в автоматизированных информационных системах. Это необходимо для обеспечения эффективной работы средств защиты информационных ресурсов. Проведение таких мероприятий сопряжено с большими финансовыми затратами, так как процесс проверки эффективности информационной безопасности является трудоемким и долгим. Эти расходы являются вполне оправданными, ведь в случае взлома информационной сети или утечки баз данных организация несет несравнимо большие убытки [5].

Произведем анализ уязвимостей объекта защиты информации при использовании информационных систем автоматизации — типового учреждения здравоохранения.

Для типового учреждения здравоохранения выявлены ниже представленные информационные активы [6].

1. Информационный актив № 1: документы, имеющие отношение к планам развития медицинского учреждения и содержащие следующую информацию:
   - информация о планах развития медицинского учреждения;
   - документация о сделках с подрядчиками;
   - медицинские программы.
2. Информационный актив № 2: документы, имеющие отношение к непосредственной деятельности медицинского учреждения:
   - персональные данные пациентов и сотрудников;
   - бюджеты, финансовая информация;
   - отчеты о работе структурных подразделений.
3. Физический актив № 1: резервные копии информационной системы медицинского учреждения.

Оценка уязвимости активов медицинского учреждения проводится в соответствии с внутренним приказом руководителя один раза в год.

Оценку проводит специальная комиссия, в состав которой входят сотрудники отдела системного админи-

Таблица 1. Результаты оценки уязвимости активов медицинского учреждения

Группа уязвимостей Содержание уязвимости	Информационный актив № 1	Информационный актив № 2	Физический актив № 1
Среда и инфраструктура			
1.1. Незащищенное хранение.			низкая
1.2. Отсутствие или некорректная политика контроля доступа.			средняя
Аппаратное обеспечение			
2.1. Подверженность влажности, пыли и загрязнению.			низкая
2.2. Подверженность перепадам температур.			низкая
2.3. Подверженность колебаниям напряжения.			низкая
Контроль доступа			
3.1. Неправильное разграничение доступа в сетях.	средняя	средняя	
3.2. Отсутствие защиты мобильного компьютерного оборудования.	низкая	низкая	
3.3. Плохое управление паролями (хранение пароля, легко угадываемые пароли и т.д.).	средняя	средняя	
Коммуникации			
4.1. Незащищенное соединение с сетями общего пользования.	средняя	средняя	
4.2. Отсутствие обновления операционных систем и программного обеспечения.	низкая	низкая	
4.3. Неконтролируемое копирование.	высокая	высокая	
4.4. Отсутствие процедур резервного копирования.	высокая	высокая	
Персонал			
5.1. Неосведомленность в вопросах безопасности	низкая	низкая	низкая
5.2. Не отменяются права доступа после увольнения	средняя	средняя	
Общие уязвимые места			
6.1. Неконтролируемая загрузки и использование программного обеспечения.	средняя	средняя	

стрирования и бухгалтерии. Данная комиссия должна своевременно идентифицировать возможные проблемы и расставить должным образом приоритеты по их предупреждению [7].

Результаты оценки уязвимости активов медицинского учреждения приведены в таблице 1.

В последние годы наметилась четкая тенденция перехода работы медицинских учреждений на цифровые технологии. Эта тенденция характерна для всех организаций вне зависимости от места их расположения.

В процессе своей деятельности такие организации пользуются информационными сетями, которые харак-

теризуются низкой степенью защиты базы данных. Сетевая структура государственных поликлиник и больниц представлена в основном различными административными и организационными связями [8].

Для обеспечения высокой степени эффективности информационного взаимодействия необходимо организовать единую корпоративную сеть учреждений. Основная задача управления сетью состоит в управлении потоками данных. Таким образом, структура сети представляет собой объект управления.

В состав информационных баз данных объектов входят различные документы. Данная информация хранится в специальных структурированных базах данных и других информационных ресурсах. Информация, хранимая в базах данных учреждений, характеризуется рядом особенностей. Информация о деятельности больниц и поликлиник, а также личные данные пациентов могут использоваться и участвовать в обмене между базами данных с определенными ограничениями [9].

Базы данных медицинских учреждений характеризуются следующими признаками [10]:

- относительно большой размер информационных ресурсов;
- постоянное обращение к информационным ресурсам со стороны большого количества пользователей;
- большое количество источников новой информации, которая стекается на единый сервер;
- необходимость осуществления множества различных операций в процессе работы с базами данных.

Базы данных, формируемые медицинскими учреждениями, как и все прочие информационные ресурсы, имеют свою классификацию [11]:

- в зависимости от источника информации;
- в зависимости от правообладателя информационных ресурсов;
- в зависимости от степени защиты и количества лиц, имеющих прямой доступ к базам данных;
- в зависимости от способа вывода информации пользователю;
- в зависимости от вида данных, хранящихся в информационной базе;
- в зависимости от формы собственности;
- в зависимости от структурных особенностей.

Всего десять лет назад медицинская система РФ характеризовалась полным отсутствием средств автоматизации обмена информацией. Все документы, с которыми приходилось ежедневно работать персоналу, имели бумажный вид. Это накладывало определенные ограничения на удобство работы с документами. Также отсутствие автоматизации документооборота сдерживало развитие и совершенствования качества обслуживания клиентов [12].

Современные информационные технологии являются полнофункциональными. Каждый работник имеет широкий набор возможностей в процессе работы с электронными базами данных пациентов. Современные масштабные многопрофильные структуры в наибольшей степени способны реализовать весь потенциал информационных технологий. К таким структурам относится многопрофильный центр здоровья.

Такие многопрофильные структуры позволяют [13]:

- осуществлять автоматизированный контроль и управление данными о всех этапах лабораторных исследований.
- осуществлять обработку данных, представленных в графическом виде.
- работа с базами данных о донорах и других пациентах, которым когда-либо проводились процедуры по переливанию крови.

Таким образом, информационные технологии позволяют врачам большее количество времени уделять пациентам, так как большой объем работы с документами осуществляется в автоматическом режиме с использованием ЭВМ. Постоянное совершенствование оборудования также диктует необходимость перехода на работу с информационными технологиями. Например, в настоящее время большинство оборудования выводит информацию о результатах исследования в цифровом виде.

Также очевиден прогресс в сфере научных исследований в результате повсеместного использования различных информационных технологий. С помощью ЭВМ появилась возможность создания сложных и емких моделей, с помощью которых осуществляется изучение различных дисциплин. С помощью информационных технологий осуществляется прогнозирование генетической предрасположенности человека к тем или иным заболеваниям [14].

Нейтрализация лишь наиболее опасных угроз достигается выбором оборонительной стратегии (в случае исключения вмешательства в процесс функционирования информационной системы). Этого можно достигнуть с помощью построения «защитной оболочки», которая подразумевает разработку неких дополнительных организационных мер, создание программных средств допуска к ресурсам ИС и использованию технических средств контроля помещений, в которых расположено критически важное оборудование.

Стратегия защиты информации от взломов подразумевает проведение комплекса следующих мероприятий: анализ контрагентов, изучение условий договоров, защита компьютерных систем и т.д. Она обеспечивает защиту информационной системы на основе постоянно действующей системы инженерно-технических мероприятий. Данная методика обеспечивает наиболее низкий уровень информационной защищенности относительно двух других методик [15].

Наступательная стратегия предусматривает активное вмешательство в деятельность известных угроз, которые могут влиять на безопасность системы. Данная методика включает в себя установку дополнительных программно-аппаратных средств аутентификации пользователей, использование более производительных технологий восстановления данных и разгрузки, а также повышение доступности системы с помощью использования резервирования.

Процессы разработки программного обеспечения для медицинских учреждений, а также его эксплуатация сопряжены с постоянными угрозами безопасности программно-аппаратного обеспечения, информационных ресурсов и персональных данных сотрудников и пациентов. Данная особенность является характерной в сфере создания программно-аппаратных продуктов, баз данных, а также других компонентов ИСПДн. Компьютерные вирусы представляют собой самые опасные средства для негативного воздействия на комплекс программно-аппаратных компонентов. Под компьютерным вирусом подразумевается ПО, предназначенное для нанесения урона базам данных. Компьютерные вирусы характеризуются возможностью распространения на другие программные продукты, и телекоммуникационные каналы.

Еще одним распространенным способом деструктивного воздействия программное обеспечение является применение алгоритмических и программных закладок. Под алгоритмической закладкой подразумевается умышленное нарушение целостности определенной части алгоритма, в соответствии с которым происходит решение задач. Также алгоритмическая закладка способная выстраивать алгоритм таким образом, чтобы в итоге отсутствовала возможность реализации алгоритма совместно с программными компонентами или комплексами. Под программной закладкой подразумеваются операторы или операнды, которые были преднамеренно включены в реализуемый код. Это осуществляется завуалировано и может произойти на любом из этапов [16].

Все известные на сегодняшний день деструктивные программные средства являются разрушительными и вредоносными. В результате их воздействия наносится колоссальный ущерб компьютерным системам и программно-аппаратным средствам. Для оценки актуальности угроз утечки информации по техническим каналам и угроз НСД необходимо определить вариант типовой модели угроз, которому соответствует рассматриваемая ИС, и оценить соответствующие типовой модели угрозы по методике определения актуальных угроз [17].

1. Угрозы утечки видовой информации.

В информационной системе больницы физическое лицо не имеет возможности неконтролируемого пребывания на территории служебных помещений, соответственно.

2. Угрозы утечки информации по каналу ПЭМИН.

3. Угрозы несанкционированного доступа к информации.

В ходе рассмотрения всех угроз, описанных в предыдущих разделах, можно сделать вывод, что главной угрозой информационной системы является угроза НСД к информации.

Актуальными угрозами исследуемого субъекта здравоохранения являются [18]:

- несанкционированный доступ к ресурсам сети с целью анализа сетевого трафика;
- несанкционированный доступ к ресурсам сети с целью сканирования параметров информационной системы;
- несанкционированный доступ к ресурсам сети с целью установки вредоносного ПО.

Потенциальных нарушителей, которые могут нанести вред информационным ресурсам и ПДн, классифицируют на нарушителей:

- внешних, которые не имеют санкционированных возможностей для объекта доступа в контролируемую зону;
- внутренних, которые имеют постоянный или разовый доступ в контролируемую зону.

Оценка рисков угроз безопасности персональных данных информационных систем медицинского учреждения проводится 1 раз в год.

Основание для проведения оценки — приказ руководителя о проведении проверки. Оценку проводят сотрудники отдела системного администрирования и бухгалтерии [19].

Результаты оценки рисков угроз безопасности персональных данных информационных систем медицинского учреждения приведены в таблице 2.

Таблица 2. Результаты оценки рисков угроз безопасности информационных систем медицинского учреждения

Группа угроз Содержание угроз	Информационный актив № 1	Информационный актив № 2	Физический актив № 1
Угрозы, обусловленные преднамеренными действиями			
1.1. Кража компьютерного оборудования и носителей информации.			низкая
1.2. Утечка конфиденциальной информации из сети по каналам связи	средняя	средняя	
1.3. Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика.	низкая	низкая	
Угрозы, обусловленные случайными действиями			
2.1. Утечка конфиденциальной информации в следствии утери мобильных устройств	низкая	низкая	
2.2. Разрушение данных по причине системного сбоя или ошибки ПО	низкая	низкая	
Угрозы, обусловленные естественными причинами (природные, техногенные факторы)			
3.1. Затопление, пожар, ураган, землетрясение и т.п.	низкая	низкая	низкая

Для перечня угроз программного характера эффективным способом противодействия является использование антивирусных средств.

Наиболее продвинутые решения в данной области предлагает компания «Лаборатория Касперского».

Лаборатория Касперского предлагает решения мирового уровня для эффективной защиты рабочих станций и серверов, блокировки вредоносного ПО, безопасности конфиденциальных данных, предотвращения неавторизованного доступа в корпоративные сети и других аспектов информационной безопасности.

К основным достоинствам этого программного продукта следует отнести [20]:

1. Управление системой можно осуществлять любым устройством, для которого имеется специальное приложение.
2. Kaspersky Endpoint Security Cloud имеет все необходимые предварительные настройки, которые освобождают сотрудников организации от наладочных работ и тестирования системы перед началом ее полноценного использования в качестве основного инструмента защиты.
3. Данный программный продукт подразумевает возможность его использования в облачном режиме, что в значительной степени расширяет его возможности.
4. Возможность использования единой учетной записи при работе под разными операционными системами.
5. Высокая степень защиты ресурсов сети за счет использования комплексного подхода при решении задач безопасности.
6. Применение инструментов для защиты мобильных устройств от попыток незаконного взлома и изменения прошивки.
7. Возможность дистанционного управления системой из головного офиса всеми филиалами.

Рассмотрим некоторые особенности предлагаемых компанией продуктов. Kaspersky Security на основе патентованных технологий и уникальной архитектуры обеспечивает надежную защиту ИС. Приложение поддерживает VMware vSphere с NSX, Microsoft Hyper-V, Citrix XenServer и KVM. Независимо от конфигурации платформы и степени гибридизации, локального или облачного расположения, вы сможете управлять системой безопасности из единой консоли. Эксперты-аналитики используют самые совершенные методы отслеживания ландшафта DDoS-угроз, опережая действия злоумышленников и обнаруживая DDoS-атаки на ранних этапах [21].

Адаптивная модель безопасности — это сочетание четырех компонентов: предотвращения, обнаружения, реагирования и прогнозирования. Это позволяет за-

метно снизить риск атак и ущерб от них — большинство угроз отражаются благодаря аналитике и превентивным технологиям, а остальные обнаруживаются и обезвреживаются гораздо быстрее, чем происходит при традиционном подходе к защите. Программный продукт Kaspersky Endpoint Security Cloud ориентирован на использование в условиях малых и средних организаций [22]. Основное назначение этого ПО — комплексная защита информационных ресурсов организации. Функционал этой системы обеспечивает управление системой дистанционно через сеть Интернет. Данный программный продукт подразумевает возможность его использования в облачном режиме, что в значительной степени расширяет его возможности. При наличии доступа в Интернет, управление системой можно осуществлять любым устройством, для которого имеется специальное приложение. Компания разработчик обеспечивает пользователей системой всей необходимой инфраструктурой для работы в облачном режиме. Программный продукт Kaspersky Endpoint Security Cloud ориентирован на использование в условиях малых и средних организаций, в которых нет полноценного штата сотрудников, которые смогли бы обеспечить работоспособность других СЗИ от НСД. В процессе разработки этого программного продукта разработчиками был сделан акцент на простоту использования и высокую эффективности защиты информационных ресурсов [23]. Таким образом, это ПО осуществляет противодействие всем известным на данный момент способам хищения информации. Kaspersky Endpoint Security Cloud имеет все необходимые предварительные настройки, которые освобождают сотрудников организации от наладочных работ и тестирования системы перед началом ее полноценного использования в качестве основного инструмента защиты. При наличии доступа в Интернет, управление системой можно осуществлять любым устройством, для которого имеется специальное приложение.

Заключение

На сегодняшний день любое медицинское учреждение оснащено оборудованием, обеспечивающем подключение этого учреждения к единой компьютерной сети. Работа с данными и обмен информацией могут осуществлять только сотрудники медицинских учреждений. Как правило, персонал имеет ограниченный доступ к ресурсам сети. Врачи имеют право доступа только к той информации, которая необходима им в процессе выполнения своих обязанностей. Все сеансы работы в сети Интернет подлежат обязательному протоколированию. Эта информация хранится на сервере и при необходимости может быть запрошена администраторами сети. В результате оснащения медицинских учреждений информационными технологиями, персонал вышел на новый качественный уровень обслуживания пациентов.

Преимущества использования информационных технологий:

- улучшение качества работы с пациентами;
- более рациональное распределение средств финансирования;
- увеличение степени эффективности работы оборудования;
- рационализация трудоемкости проводимых мероприятий;
- возможность обмена информацией в процессе работы между персоналом в режиме реального времени.

По завершению написания статьи все поставленные задачи решены, цель работы достигнута.

ЛИТЕРАТУРА

1. Афанасьев Э.В., Ярошенко В.Н. Информационная безопасность. — М.: Экономика, 2019. — 478 с.
2. Алтухова, С.О. Программирование в среде Delphi: разработка баз данных / С.О. Алтухова, З.А. Кононова; Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского. — Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2020. — Ч. 2. — 52 с.
3. Беленькая М.Н., Малиновский С.Т., Яковенко Н.В. Администрирование в информационных системах. Научно-популярное издание. — М.: Горячая линия — Телеком, 2020. — 300 с.
4. Бова, В.В. Основы проектирования информационных систем и технологий: учебное пособие / В.В. Бова, Ю.А. Кравченко; Южный федеральный университет, Инженерно-технологическая академия. — Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. — 106 с.
5. Буза, М.К. Архитектура компьютеров: учебник / М.К. Буза. — Минск: Вышэйшая школа, 2019. — 416 с.
6. Вейцман В.М. Проектирование информационных систем: Учебное пособие. — М.: МУБИНТ, 2021. — 214 с.
7. Гвоздева В.А. Информатика, автоматизированные информационные технологии и системы: учебник / В.А. Гвоздева. Москва: Форум: Инфра-М, 2020. — 541 с.
8. Гохберг Г.С. Информационные технологии: Учебник для студ. учрежд. сред. проф. образования / Г.С. Гохберг, А.В. Зафиевский, А.А. Короткин. — М.: ИЦ Академия, 2019. — 208 с.
9. Есаулова С.П. Информационные технологии в туристической индустрии: Учебное пособие / С.П. Есаулова. — М.: Дашков и К, 2021. — 152 с.

10. Ибрагимов И.М. Информационные технологии и средства дистанционного обучения: Учебное пособие для студ. высш. учеб. заведений / И.М. Ибрагимов; Под ред. А.Н. Ковшов. — М.: ИЦ Академия, 2020. — 336 с.
11. Илюшечкин В.М. Основы тестирования информационных систем. — М.: Юрайт, 2020. — 224 с.
12. Ипатова, Э.Р. Методологии и технологии системного проектирования информационных систем: учебник / Э.Р. Ипатова, Ю.В. Ипатов. — 2-е изд., стер. — Москва: ФЛИНТА, 2019. — 257 с.
13. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика: учебное пособие / В.Я. Ищейнов. — Москва; Берлин: Директ-Медиа, 2020. — 271 с.
14. Ковган, Н.М. Компьютерные сети: учебное пособие / Н.М. Ковган. — Минск: РИПО, 2021. — 180 с.
15. Криницкий Н.А., Миронов Г.Д., Фролов Г.Д. Расчет экономической эффективности информационных систем — М.: Наука, 2020. — 384 с.
16. Кугаевских, А.В. Проектирование информационных систем. Системная и бизнес-аналитика: учебное пособие / А.В. Кугаевских; Новосибирский государственный технический университет. — Новосибирск: Новосибирский государственный технический университет, 2020. — 256 с.
17. Маглинец Ю.А., Анализ требований к автоматизированным информационным системам. — 2019.
18. Малявко, А.А. Суперкомпьютеры и системы. Построение вычислительных кластеров: учебное пособие / А.А. Малявко, С.А. Менжулин; Новосибирский государственный технический университет. — Новосибирск: Новосибирский государственный технический университет, 2019. — 96 с.
19. Маслов, А.В. Проектирование информационных систем в экономике: Учебное пособие / А.В. Маслов. — Т.: Томский политехнический университет, 2018. — 216 с.
20. Моргулец, О.Б. Менеджмент в сфере услуг: Учебное пособие / О.Б. Моргулец. — К.: Центр учебной литературы, 2020. — 384 с.
21. Коберн, А. Современные методы описания функциональных требований к системам: Учебник / А. Коберн. — М.: Лори, 2019. — 263 с.
22. Корячко В.П., Таганов А.И. Процессы и задачи управления проектами информационных систем./М.: Горячая линия-Телеком, 2021. 376 с.
23. Коберн, А. Современные методы описания функциональных требований к системам: Учебник / А. Коберн. — М.: Лори, 2020. — 263 с.
24. Кугаевских, А.В. Проектирование информационных систем. Системная и бизнес-аналитика: учебное пособие / А.В. Кугаевских; Новосибирский государственный технический университет. — Новосибирск: Новосибирский государственный технический университет, 2019. — 256 с.
25. Основы информационной безопасности учебник / В.Ю. Рогозин, И.Б. Галушкин, В. Новиков, С.Б. Вепрев; Академия Следственного комитета Российской Федерации. — Москва: Юнити-Дана: Закон и право, 2020. — 287 с.
26. Программная инженерия: учебное пособие / сост. Т.В. Киселева; Северо-Кавказский федеральный университет. — Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2020. — Ч. 1. — 137 с.

Журнал «Современная наука: актуальные проблемы теории и практики»

Российский экономический университет им. Г.В. Плеханова