Тип работы: Дипломная работа

Предмет: Информационные технологии

Введение

Темой дипломного проекта является организация защиты информации в медицинских информационных системах на примере Полное юридическое наименование: бюджетное учреждение здравоохранения Омской области "Городская больница № 6" далее БУЗОО «ГБ №6»
На сегодняшний день системы защиты информации очень востребованы как среди государственных, так и

среди коммерческих организаций. Системы информационной безопасности нуждаются в надежной защите ввиду повсеместно распространившихся краж информации, превратившихся в проблему мирового масштаба.
Серьезность и острота проблемы потребовали от органов государственной власти принятия конкретных мер по ее урегулированию. В 2007 году в России вступил в силу Федеральный закон (ФЗ) «О персональных данных»[1], направленный на обеспечение всех необходимых мер по защите информации, используемой коммерческими и государственными организациями.
В соответствии с 152–ФЗ, каждое предприятие должно обеспечить защиту персональных данных своих сотрудников, клиентов и партнеров и принять все необходимые меры во избежание следующих правонарушений:
– кража персональных данных;
– изменение;
– блокирование;
– копирование;
– разглашение информации и другие незаконные действия, указанные в 152–ФЗ.
Поскольку под понятие «Персональные данные» попадают такие данные о человеке, как фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, информация о доходах и многое другое – система защиты персональных данных нужна фактически любой организации. В случае нарушения положений закона № 152–ФЗ о защите персональных данных компания может быть привлечена к судебному разбирательству (вплоть до приостановления действий, аннулирования соответствующих лицензий), а виновные лица – к гражданской, уголовной, административной, дисциплинарной ответственности. Согласно закону № 152–ФЗ, информационные системы персональных данных должны были быть приведены в соответствие с требованиями законодательства не позднее 1 января 2011 года.
На сегодняшний день в БУЗОО «ГБ №6» не реализована система защиты персональных данных, поэтому существующая система информационной безопасности организации подвергается серьезному риску. Реализация системы защиты персональных данных в организации позволит значительно снизить вероятность возникновения ситуаций по неправомерному доступу к информации организации.
Целью дипломного проекта является непосредственная модернизация существующей системы информационной безопасности в БУЗОО «ГБ №6.
Для достижения поставленной цели необходимо первоначально решить следующие задачи:
• Анализ правовой основы защиты персональных данных;
• Анализ деятельности организации
• Описание информационной системы компании, используемой для обработки и хранения персональных данных;
• Построение модели угроз персональных данных;
• Разработка мер по защите персональных данных;
• Оценка рисков
• Обоснование экономической эффективности системы защиты персональных данных в локально вычислительной сети;
Главной функцией разрабатываемой системы является встраивание защиты персональных данных в существующую в организации систему информационной безопасности.

I Аналитическая часть

1.1. Технико–экономическая характеристика предметной области и предприятия (Установление границ рассмотрения)

1.1.1. Общая характеристика предметной области

Фонд социального страхования Российской Федерации (далее Фонд или РОФСС) является специализированным финансово–кредитным учреждением при Правительстве Российской Федерации. Фонд осуществляет свою деятельность в соответствии с Конституцией Российской Федерации, законами Российской Федерации, указами Президента Российской Федерации, утвержденными Постановлением Правительства РФ от 12 февраля 1994 года № 101.
В Фонд социального страхования Российской Федерации входят следующие исполнительные органы:

региональные отделения, управляющие средствами государственного социального страхования на территории субъектов Российской Федерации; филиалы отделений, создаваемые региональными отделениями Фонда по согласованию с председателем Фонда.
Основными задачами Фонда являются:
– осуществление государственного социального страхования на случай временной нетрудоспособности и в связи с материнством;
– осуществление обязательного социального страхования от несчастных случаев на производстве и профессиональных заболеваний;
– участие в реализации федеральных государственных программ, направленных на охрану здоровья граждан и улучшение их социально–экономического положения;
– осуществление мер, обеспечивающих финансовую устойчивость Фонда;
Для осуществления данных видов деятельности организации необходима информационная система (ИС). Функциональное предназначение ИС такой организации заключается в работе с информацией: ввод и вывод, хранение или уничтожение, обработка и перераспределение, а также передача между составными элементами ИС и глобальной сети, то есть автоматизация проведения рабочих операций, обеспечение быстроты, надежности и безопасности.
Рабочий процесс организации состоит из следующих частей:
Ввод информации. На данном этапе осуществляется выполнение следующих функций, требующих автоматизации с использование ИС:
– учет и регистрация страхователей ;
– прием отчетов от страхователей.
Информация в организацию поступает следующим образом. Страхователь для регистрации заполняет заявление утвержденного образцами представляет свои паспортные данные, сведения о государственной регистрации, сведения о выданных лицензиях, данные по трудовому договору, адрес места осуществления деятельности, счет в кредитной организации, контактная информация и некоторые другие необходимые документы, а также копии следующих документов: свидетельства о государственной регистрации физического лица в качестве индивидуального предпринимателя; свидетельства о постановке на учет в налоговом органе; трудовые книжки нанимаемых им работников; трудовых договоров, заключенных с работниками.
Заявление принимается на бумажном носителе информации. Далее информация поступает на АРМ учета и регистрации юридических и физических лиц, где по каждому заявлению создается и оформляется электронный документ страхователя, после чего информация помещается в единую базу данных.

При приеме отчетности происходит аутентификация отправителя, проверка правильности сумм страховых ежеквартальных взносов и точность заполнения форм. База данных по страхователю дополняется данными по результатам страховых взносов за отчетные периоды. Данные по отчетности поступают в РФСС от страхователей, равно как и от сторонних организаций (отделений пенсионного фонда, служб судебных приставов, центров занятости, территориального фонда обязательного медицинского страхования, казначейство), как на бумажных носителях, так и в электронном виде по защищенным каналам связи, например Контур–Экстерн, VipNet, Dipost, СПРИНТЕР. Либо курьером, который передает от организации в РФСС специальным образом опечатанный конверт. Прием информации по каналам связи осуществляется на АРМ, оборудованных соответствующими программными средствами. Прием информации осуществляют пользователи соответствующих АРМ.
Ввод и последующая обработка персональных данных осуществляется сотрудниками организации (пользователями АРМ отдела регистрации, проверки, кадров, юридического и др.) с использованием программных и аппаратных средств, руководствуясь нормативной и организационной – распорядительной документации в каждом из перечисленных отделов. Информация на выходе процесса обработки может принимать как электронный вид (заполненные заявления, разнообразные бланки, формы, приказы, распоряжения и т.п.), так и бумажный (заполненные заявления, разнообразные бланки, формы, приказы, распоряжения, личные дела и т.п.). Информация в конечном виде хранится на сервере БД, архиве.
Доступ к информации осуществляется в соответствии с рабочими обязанностями пользователей (операторами АРМ) на их рабочих местах.
На данном этапе выполняются такие функции, требующие автоматизации с использованием ИС как:
– начисление платежей от страхователей;
– проведение проверок и соответствий по выплатам страхователей;

– контроль над поступлением страховых выплат организациям;
– формирование отчетности в центральный фонд социального страхования;
– организация работы вспомогательных служб (отдела кадровой и юридической работы, бухгалтерия).
– проведение анализа и составление экономической статистики фонда.
Выполнение перечисленных функций осуществляется на АРМ сотрудников контроля документооборота, бухгалтерии, статистического отдела и экспертизы и других АРМ.
При этом информация (как обработанная, так и еще не подвергшаяся обработке) перемещается по следующим основным направлениям:
– АРМ регистрационного отдела – Информационный сервер БД, Файловый сервер и обратно;
– АРМ отдела контроля документооборота – Сервер БД, Файловый сервер и обратно;
– АРМ приема и передачи информации для сторонних организаций по защищенным каналам связи – глобальной сети и обратно;
Доступ к информации находящейся и использующейся внутри организации могут получить только сотрудники, связанные с выполнением бизнес – функции организации, в установленном в организации порядке. Наряду с электронными средствами обработки информации в организации так же применяется и ручная обработка информации. Например: поиск информации в архивах; перенос информации, зафиксированной на бумажном носителе, с одного рабочего места на другое, перевод документов в электронный вид и наоборот, а также работа с внутриорганизационными отчетами.
Работа с информацией осуществляется непосредственно на АРМ, рабочих станциях (РС). При этом используется аппаратура этих мест (персональные компьютеры и другие средства обработки информации), с установленными программными средствами и оборудованием прошедшем сертификацию.
На этапе обработки происходит модификация (добавление, редактирование, удаление) учетных записей о страхователе. В автоматическом режиме, при помощи программного обеспечения производятся расчеты (страховых выплат, взносы страховщиков, расчет пени и др.).
Далее выполняется сохранение новых данных в БД, при этом данные проходят проверку программными средствами, на соответствие установленным нормам. Также возможно удаление данных из БД учетных записей о страхователе, в этом случае данная операция также проходит проверку на соответствие установленным нормам.
Кроме обработки данных страхователей, происходит хранение и обработка персональных данных сотрудников самой организации (отдел кадровой и юридической работы, отдел бухгалтерского учета, отдел по техническому и хозяйственному обеспечению).
Вывод информации. После процесса обработки обработанная информация распространяется от сотрудника, осуществившего эту обработку, по сети и определенным образом может быть доступна любому другому пользователю, тем или иным образом связанным с реализацией бизнес – функции организации, в установленном порядке.
Информация, прошедшая обработку распространяется по направлениям, перечисленным выше.
Дальнейшее хранение, модификация и/или уничтожение информации может осуществляться как и на рабочих станциях, так и на сервере. А также обработанная информация по сетям защищенной связи распространяется в сторонние организации (отделения пенсионного фонда, службу судебных приставов, центры занятости, налоговые инспекции, территориальный фонд обязательного медицинского страхования, казначейство, и т.п.).
Как выходную информацию можно рассматривать различные сертификаты, свидетельства, заполненные бланки и формы установленного образца, отчетные документы, приказы, распоряжения и т.д. и т.п.

1.1.2. Организационно–функциональная структура предприятия

При реализации организационной структуры управления БУЗОО «ГБ №6 требуется реализовать эффективное распределение управленческих функций по отделам. При этом требуется выполнить следующий ряд условия:
– решение одних и тех же вопросов не должно находиться в компетенции нескольких отделов;
– в должностные обязанности начальников отделов должны быть включены все функции управления, существующие в отделе;
– на данный отдел не должно быть возложено решение вопросов эффективно решаемых в другом отделе.
Между отделами организации существуют как горизонтальные, так и вертикальные связи.
Горизонтальные связи характеризуются равноправием элементов, например, связь между начальниками

отделов в одной организации.
Вертикальные связи, в отличие от горизонтальных, характеризуются подчинением вышестоящему звену, например, связь между начальником отдела и сотрудниками данного отдела.
Основу управленческой структуры организации составляет определенная система. Существуют три основные системы управления организацией:
– Линейная, определенная схемой прямого подчинения по всем вопросам нижестоящих отделов вышестоящим. Данная система достаточно проста и может быть эффективна, если не велико число рассматриваемых вопросов и по ним могут быть даны решения в ближайших отделах
– Функциональная, представляющая схему подчинения нижестоящего отдела ряду функциональных отделов, решающих определенные управленческие вопросы. При данной системе управления указания поступают более квалифицированные. Однако подчиненные отделы не всегда знают, как согласовать полученные указания, в какой очередности их выполнять. Именно поэтому данный вид управления практически применяется крайне редко.
– Смешанная, определяется определенными комбинациями функций линейного и функционального управления.
Административные структуры располагают множеством признаков, которые могут быть приложены в качестве критериев их группировки. Проводят различия структур простых и сложных, жестких и гибких, линейных и функциональных, постоянных и переменных, типовых и индивидуальных, формальных и неформальных, сложившихся и экспериментальных, централизованных и децентрализованных и т.д. Можно классифицировать структуры устойчивые и неустойчивые, надежные и ненадежные, бюрократические и демократические, дорогие и дешевые и т. д.
Схема организационно–штатной структуры БУЗОО «ГБ №6 представлена на рисунке 1.

Рисунок 1. Организационно–штатная структура БУЗОО «ГБ №6
Планово–экономический отдел осуществляет планирование финансово–хозяйственной деятельности, проводит работу по совершенствованию организационных структур, штатных расписаний в соответствии со схемами должностных окладов и установленным фондом заработной платы и организацию статистического учета, разрабатывает локальных актов экономической направленности (положения о системе оплаты труда, ценообразования и т.д.).
Отдел финансов, бухгалтерского учета и отчетности, являясь структурным подразделением отделения Фонда, посредством ведения бухгалтерского учета формирует полную и достоверную информацию о деятельности отделения Фонда по всем его направлениям и его имущественном положении.
Данная информация необходима для осуществления контроля за исполнением бюджета отделения Фонда и сметы на его содержание, а также для составления установленной отчетности и предоставления различной оперативной информации.
Отдела информационных технологий и безопасности информации проводит анализ и изучение проблем обслуживания автоматизированных систем Управления, проводит контроль состояния и безопасности сети и сетевого оборудования.
Отдел страхования на случай временной нетрудоспособности и в связи с материнством выплату пособий по временной нетрудоспособности (оплата «больничных»), пособий по беременности и родам, единовременных пособий при постановке на учет в ранние сроки беременности, единовременных пособий при рождении, ежемесячных пособий по уходу за ребенком.
Отдел организационно-кадровой работы осуществляет организационно–кадровое, информационно-аналитическое обеспечение деятельности.

1.2. Анализ рисков информационной безопасности

1.2.1 Идентификация и оценка информационных активов

Информационная безопасность обеспечивается использованием технических средств [15]:
• построения модели защищенной системы;
• управления доступом к ресурсам системы;
• обеспечения целостности и конфиденциальности;

• обеспечения наблюдаемости;
• защиты от воздействий вирусов и иных воздействий, вызывающих любую несанкционированную модификацию информации;
• защиты информации при передаче информации.
Главной задачей технических средств защиты информации является предотвращение умышленного или случайного несанкционированного доступа к информации и ресурсам (с целью ознакомления, использования, модификации или уничтожения информации) со стороны сотрудников организации или посторонних лиц, которые находятся в пределах зон безопасности информации, независимо от способа доступа к этим зонам.
Взаимодействие ТС должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами должны располагаться в пределах контролируемой зоны.
Наиболее значимыми для защиты информации являются программные средства защиты, позволяющие создавать модель защищенной информационной среды с построением правил разграничения доступа, централизовано управлять процессами защиты, интегрировать различные механизмы и средства защиты в единую систему, создавать достаточно удобный, интуитивно доступный пользовательский интерфейс администратора безопасности. Причем, с учетом сложности автоматизированной системы, а также необходимости именно комплексного и эффективного использования всех автоматизируемых средств защиты информации, обеспечения высокой управляемости ими, значительную часть этих средств целесообразно выделять в автономный комплекс средств защиты информации, в его специфичную функциональную компоненту или подсистему.
Данная подсистема, как одна из основных в системе технической защиты информации, должна обеспечивать сохранение основных функциональных свойств защищенной информации (целостность, конфиденциальность, доступность и наблюдаемость).
Оценка способности системы обеспечивать каждое из этих функциональных свойств, производится по сформулированной в нормативных документах по защите информации системе критериев оценки защищенности. Состав средств защиты информации и их вклад в обеспечение функциональных свойств защищаемой системы представлены на рисунке 2.

Рисунок 2. Состав средств защиты информации

Идентификация информационных ресурсов должна быть выполнена в отношении поименованных информационных объектов (массивов и баз данных, документов и массивов документов, сообщений и т. д.) с учетом выявления сведений по их владению и использованию.
Целесообразно выделить характеристические показатели (признаки) использования [17]:
• в функциональных подсистемах (прикладных сервисах) АС и автоматизированных задачах функциональных подсистем, для решения которых необходима информация из этих информационных объектов;
• в подразделениях и службах (возможно, с указанием должностей), в интересах которых решаются автоматизированные задачи;
• в удаленных объектах ОИ (площадки, представительства и т. д.) (наименование, место расположения объекта).
Обязательным характеристическим показателем информационного объекта должен быть уровень конфиденциальности.
Категорирование информационных активов организации является необходимым элементом организации работ по обеспечению информационной безопасности БУЗОО «ГБ №6, целями которого является:
• создание нормативно–методической основы для дифференцированного подхода к защите ресурсов БУЗОО «ГБ №6, (информации, задач, специализированных АРМ, рабочих станций);
• выработка типовых решений по принимаемым организационным мерам защиты и распределению аппаратно–программных средств защиты для различных категорий рабочих станций БУЗОО «ГБ №6.
Активы БУЗОО «ГБ №6» делятся на 2 класса:
• информационные ресурсы;
• аппаратные ресурсы.
В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов введены четыре требуемых категории доступности информации [23].

«Беспрепятственная доступность» — доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не должна превышать нескольких секунд или минут).
«Высокая доступность» — доступ должен осуществляться без существенных задержек по времени (задача решается ежедневно, задержка получения результата не должна превышать нескольких часов).
«Средняя доступность» — доступ может обеспечиваться с существенными задержками по времени (задача решается раз в несколько дней, задержка получения результата не должна превышать нескольких дней).
«Низкая доступность» — задержки по времени при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата — несколько недель).
Для обеспечения уровнями безопасности различных видов аппаратных ресурсов, используемых в организации, вводятся следующие категории.
Категории отказоустойчивости:
«Высшая» — к данной категории относятся критически важные аппаратные средства (Сервер СУБД и дисковые массивы, содержащие базу данных ЕИИС (единой интегрированной информационной системы), сервер – контроллер домена, файловый сервер, сервера технологических процессов, маршрутизаторы, коммутаторы, межсетевые экраны). К высшей категории отказоустойчивости относятся также компьютеры с установленными средствами криптографической защиты информации.
«Средняя» — к данной категории относятся рабочие станции пользователей. Непрерывность технологических процессов обеспечивается наличием резервных рабочих станций.
«Низшая» — к данной категории относятся концентраторы и офисная техника.
Категории доступа:
«Строго ограниченный» — физический доступ к данной категории средств вычислительной техники регламентируется приказами руководства Организации, инструктивными и регламентирующими документами. К данной категории относятся ЭВМ с установленными средствами криптографической защиты информации, сервер СУБД и дисковые массивы, содержащие базу данных ЕИСС, сервер – контроллер домена, файловый сервер, сервера технологических процессов, маршрутизаторы, коммутаторы, межсетевые экраны.
«Ограниченный» — к данной категории относятся рабочие станции пользователей и средств вычислительной техники, доступ к которым регламентируется должностными инструкциями сотрудников Организации.
Каналы связи, используемые в технологических процессах, не категорируются.
Перечень активов, подлежащих защите, приведен в таблице 1.

Таблица 1
Оценка информационных активов БУЗОО «ГБ №6
Вид деятельности Наименование актива Форма предоставления актива Владелец актива Критерии определения стоимости Размерность оценки
Количественная оценка (тыс. руб.) Качественная оценка
Информация о фактах и параметрах нетрудоспособности граждан, используемая для назначения и выплаты пособий Сведения о фактах и параметрах нетрудоспособности граждан Информация на носителях и в линиях связи, он–лайн–сервисах Руководитель организации, Отдел страхования на случай временной нетрудоспособности и в связи с материнством, Отдел страхования профессиональных рисков Репутация организации, результаты финансовой деятельности 1000 высокая
Учетная информация об инвалидах Сведения о назначении выплат инвалидам Информация на носителях и в линиях связи, он–лайн–сервисах Руководитель организации, Отдел страхования профессиональных рисков Репутация организации, результаты финансовой деятельности 500 высокая
Расчетно–кассовое обслуживание Сведения об остатках средств на лицевых счетах Информация на носителях и в линиях связи, он–лайн–сервисах Руководитель организации, кассиры Репутация организации, результаты финансовой деятельности 1000 высокая
Операции с пластиковыми картами Персональные данные сотрудников Информация на носителях и в линиях связи, бумажных документах Руководитель организации, сотрудники бухгалтерии Репутация организации, результаты финансовой деятельности 1000 высокая

Список литературы

1. Федеральный закон РФ от 27 июля 2006 года № 152–ФЗ «О персональных данных» (ред. от 04.06.2014)
2. Фролова П.С., Егорова Л.С., Фролова О.Н. Стратегия управления кадровой безопасностью организации // Генезис экономических и социальных проблем субъектов рыночного хозяйства в России: Научное издание. Выпуск VII / ИГТА. Иваново, 2013. 308 с. С. 53–61.
3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197–ФЗ (ред. от 24.11.2014)
4. Алавердов А.Р. Управление кадровой безопасностью организации – М.: Маркет ДС, 2010. – 176 с.
5. Сальникова Л. В. Ошибки работодателя, сложные вопросы применения Трудового кодекса РФ – М.: Омега–Л, 2012. – 152 с.
6. Кириллов А. Соблюдение принципов управления в кадровом делопроизводстве. //Кадровик. 2014. №9. С. 102–109.
7. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
8. Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. №55/86/20 «Об утверждении порядка проведения классификации ИС персональных данных»
9. Приказ Федеральной службы по техническому и экспортному контролю от 5.02.2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в ИСах персональных данных»
10. Базовая модель угроз безопасности персональных данных при их обработке в ИСах персональных данных. Утверждена ФСТЭК России 15.02.2008 г.
11. Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСах персональных данных. Утверждена ФСТЭК России 14.02.2008 г.
12. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в ИСах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/5–144
13. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в ИСах персональных данных. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/6/6–622
14. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
15. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты – Екатеринбург: УрФУ, 2012. – 235 с.
16. Горевая М.И., Клочков Г.А., Курчеева Г.И. Экономическая эффективность проектных решений. Учебное пособие по дипломному проектированию. – М: Изд–во: Московская академия предпринимательства при Правительстве Москвы, 2012. – 156 с.
17. Домарев В.В. "Безопасность информационных технологий. Системный подход" – К.:ООО ТИД «Диасофт», 2013. – 992 с.
18. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2013. – 212 с.
19. Шаньгин В. Информационная безопасность и защита информации – М.: ДМК Пресс, 2014. – 702 с.
20. Крайнова О. Управление предприятиями в сфере информационных технологий — М.: ДМК Пресс, 2013. – 144 с.
21. Лапонина О. Р. Межсетевое экранирование. – М.: Бином, 2012. –354 с.
22. Гришина Н. Информационная безопасность предприятия. Учебное пособие – М.: Форум, 2015. – 240 с.
23. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов.– М.: Горячая линия–Телеком, 2012. – 280 с.
24. Девятин П. Модели безопасности компьютерных систем. Управление доступом и информационными потоками – М.: Горячая линия–Телеком, 2013.– 338 с.
25. Сборник статей. А.Ю.Щеглов, К.А.Щеглов. Под общим названием «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ. Новые технологии, методы и средства добавочной защиты информации от несанкционированного доступа (НСД)». – СПб.: Питер, 2012. – 187 с.
26. Селезнева Н.Н., Ионова А.Ф. Финансовый анализ. Управление финансами: Учеб.пособие для вузов. – 2–е изд., перераб. и доп. – М.: ЮНИТИ–ДАНА, 2013. – 639 с.

27. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности – СПб: Питер, 2014.– 320 с.
28. Торокин А. А. Инженерно–техническая защита информации – М: Гелиос АРВ, 2012. – 449 с.
29. Бирюков А. Информационная безопасность. Защита и нападение– М.: ДМК Пресс, 2008. – 320 с.
30. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – М.: Юниор, 2012. – 474 с.
31. Щеглов А.Ю., Защита компьютерной информации от несанкционированного доступа. – М.: Наука и техника, 2013. – 384 с
32. Яковлев В.В., Корниенко А.А. Информационная безопасность и защита информации в корпоративных сетях банковского сектора. – М., 2014. – 327 с.
33. Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Международные отношения, 2013. – 400 с.