Содержание:

Введение

Обеспечение информационной безопасности – одна из важнейших задач любого предприятия, работающего с информацией, разглашение которой может повредить его деятельности. Примечательным в данной работе является то, что каждый человек понимает необходимость защиты информации, но на практике лишь малая доля из них действительно представляет себе возможные последствия и методы их предотвращения. В сознании большинства людей представление о информационной угрозе складывается в основном из художественных фильмов и телесериалов о «хакерах». На практике же работа по обеспечению информационной безопасности должна учитывать множество факторов, связанных с каждым конкретным защищаемым объектом.

С каждым годом скорость появления новых научных открытий неуклонно растет, особенно в сфере информационных технологий. Появляются новые технологии обработки информации, ее хранения, передачи, благодаря чему растут и вычислительные мощности, которые можно направить на преодоление даже самых сложных систем защиты. Развитие физики волн, увеличение чувствительности оборудования, фиксирующего электромагнитные волны, радиоволны порождает все более изощренные методы получения информации, даже не получая непосредственного доступа к компьютеру жертвы.

В российском обществе, где еще со времен начала 90-х практика использования противоправных средств при ведении бизнеса стала скорее нормой, чем отклонением от нее, угроза информационной безопасности стоит особо актуально. Поэтому администратору необходимо постоянно следить за появлением новых методов в области взлома, прослушивания каналов связи и защитного программного обеспечения.

Объектом исследования данной работы является информационная безопасность, предметом – угрозы информационной безопасности.

Цель работы – рассмотреть виды и состав угроз информационной безопасности.

Для достижения поставленной цели необходимо выполнить ряд задач:

- рассмотреть основные понятия по информационной безопасности;
- исследовать классификацию угроз информационной безопасности;
- провести анализ угроз информационной безопасности;
- рассмотреть методы защиты от угроз.

В процессе работы была применена совокупность методов экономико-статистического анализа, методы синтеза и анализа экономической информации.

1 Виды угроз информационной безопасности

1.1 Основные понятия по информационной безопасности

Информация[1] - сведения (сообщения, данные) независимо от формы их представления. Информация может быть представлена как на материальном носителе в виде символов, знаков, рисунков с возможностью ее визуального просмотра (документированная информация), так и в электронном виде с возможностью ее просмотра только с использованием программно-технических средств. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне».

Защита информации от несанкционированного доступа – деятельность (работа) должностных лиц, направленная на создание и поддержание условий, установленных требованиями нормативных документов, исключающих НСД к защищаемой (подлежащей защите) информации. Под защищаемой информацией понимаются информационные ресурсы и программное обеспечение, подлежащие защите.

Защите подлежит информация любого вида, доступ к которой ограничивается. Ограничение доступа к информации устанавливается федеральными законами и нормативными актами для защиты основ конституционного строя, здоровья, нравственности, прав и законных интересов других лиц [13, с.102].

Объект – автоматизированная или компьютерная система обработки данных.

Субъект – любая сущность, которая способна инициировать выполнение операций над объектами.

Доступ – категория субъектно-объектной модели, которая описывает процесс выполнения операций субъектов над объектами.

Автоматизированная система обработки информации (АС) – это организационно-техническая система, которая включает следующие взаимосвязанные компоненты:

- технические средства передачи и обработки данных (средства вычислительной техники и связи);
- методы и алгоритмы обработки в виде соответствующего ПО;
- информация (массивы, наборы, базы данных) на различных носителях;
- персонал и пользователи системы, объединенные по тематическому, организационно-структурному, технологическому или другим признакам для выполнения автоматизированной обработки данных (информации) для удовлетворения потребности в информации субъектов информационных отношений.

Утечка защищаемой информации – ее неконтролируемое разглашение, несанкционированный доступ к ней, получение защищаемой информации разведками [12, с.89].

Хищение информации – несанкционированный доступ к информации, повлекший ознакомление с ней недопущенных субъектов. При этом возможно как полное хищение, когда похищаемая информация на машинном носителе информации полностью уничтожается, так и хищение, при котором производится только копирование защищаемой информации.

Несанкционированное уничтожение защищаемой информации – процесс обработки информации не допущенным к ней субъектом, в результате которого защищаемая информация удаляется с машинного носителя информации без возможности ее дальнейшего восстановления.

Несанкционированная модификация защищаемой информации – ее несанкционированное искажение, влекущее за собой изменение смысла, состава, содержания, реквизитов и характеристик защищаемой информации.

Несанкционированное копирование защищаемой информации – производимый в нарушение правил разграничения доступа процесс переноса защищаемой информации с одного машинного носителя информации на другой.

Несанкционированное блокирование защищаемой информации – процесс обработки информации, в результате которого доступ к защищаемой информации допущенным к ней субъектам становится невозможным.

При отсутствии средств регистрации и учета процессов копирования, уничтожения и модификации защищаемой информации установить факт таких событий безопасности крайне затруднительно.

Несанкционированный доступ к информации – доступ к информации, нарушающий установленные (принятые) нормативными правовыми актами требования (правила, порядок) разграничения доступа с использованием штатных средств (механизмов, методов, способов, возможностей), предоставляемых средствами ВТ.

1.2 Классификация угроз информационной безопасности

Под угрозой информационной безопасности (ИБ) понимается совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее [9, с.67].

В общем случае угроза ИБ может характеризоваться следующими параметрами:

- источник угрозы;
- используемая уязвимость;
- способ реализации угрозы;
- деструктивные действия, выполняемые при реализации угрозы [8, с.102].

Угрозы безопасности могут присутствовать на любом уровне иерархии, начиная от физической безопасности и заканчивая любым логическим доступом к информации. Для определения угроз безопасности рассматриваются все уровни, на которых может быть получен доступ к активам. Неспроста процессы обеспечения информационной безопасности рассматриваются как противоборство собственника и злоумышленника за контроль над информационными активами. На этом этапе разрабатывается модель угроз и нарушителей, в которой и описываются все виды угроз.

Рассмотрим самые распространенные угрозы, с которыми могут столкнуться современные информационные системы. Исследование теоретических аспектов о возможных угрозах, а также о наиболее уязвимых местах, которые эти угрозы, как правило, эксплуатируют, важно по той причине, что на основе подобной информации можно выбрать наиболее экономичные средства для обеспечения безопасности. Существует множество мифов в сфере информационных технологий, и недостаток знаний в этой области может привести к перерасходу средств и, что намного хуже, к концентрации ресурсов в тех местах, где в них нет особой надобности, при одновременном ослаблении действительно уязвимых направлений.

Следует подчеркнуть, что само понятие «угроза» зачастую по-разному трактуется в той или иной ситуации. Так, для подчеркнуто открытой организации угроз конфиденциальности данного определения может вовсе не существовать - вся информация априори считается общедоступной; однако, как правило, нелегальный доступ является серьезной опасностью. Иными словами, угрозы, как и все в сфере информационного обеспечения, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Угрозы можно классифицировать по различным критериям, среди которых:

- отдельные аспекты информационной безопасности (целостность, доступность, конфиденциальность);
- компоненты информационных систем, на которые нацелены угрозы (данные, аппаратура, программы, поддерживающая инфраструктура);
- способ осуществления (случайные/преднамеренные действия или действия природного/техногенного характера);
- расположение источника угроз (внутри/вне рассматриваемой информационной системы).

Наибольшее распространение имеют угрозы первого типа. К ним относятся непреднамеренные ошибки штатных сотрудников, системных администраторов, операторов и других лиц, занимающихся обслуживанием информационных систем.

Другие угрозы доступности классифицируем по компонентам информационных систем, на которые нацелены угрозы:

- отказ пользователей;
- отказ поддерживающей инфраструктуры;
- внутренний отказ информационной системы.

Как правило, применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (зачастую проявляется при необходимости исследования новых возможностей и при расхождении между запросами пользователей и реальными возможностями и техническими характеристиками);
- невозможность работать с системой из-за отсутствия соответствующей подготовки (неумение интерпретировать диагностические сообщения, недостаток общей компьютерной грамотности, неумение работать с документацией и пр.);
- невозможность работать с системой из-за отсутствия технической поддержки (недостаток справочной информации, неполнота документации и т.п.).

Основными источниками угроз безопасности информации являются:

- угрозы по каналам утечки вещественной информации (незаконный доступ к физическим объектам защиты);
- угрозы утечки информации по техническим каналам;
- угрозы НСД к данным, обрабатываемым в локальной сети.

Угрозы утечки информации по техническим каналам включают в себя[13]:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН (Побочные Электромагнитные Излучения и Наводки).

Наиболее значимыми угрозами безопасности информации для компании (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную или коммерческую тайну, а также персональных данных;
- нарушение функциональности компонентов информационной системы, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов, а также фальсификация (подделка) документов.

2 Состав угроз информационной безопасности

2.1 Современное состояние угроз информационной безопасности

Обзор компьютерных преступлений приведен на основе исследования, проведенного аналитическим центром компании InfoWatch. Были исследованы утечки конфиденциальной информации за 2015 год. По данным исследования, по сравнению с прошлым годом количество утечек информации в мире выросло на 7,8%, число «российских» утечек по сравнению с данными 2014 года сократилось на 28,1%.

За 2015 год Аналитический центр InfoWatch зарегистрировал 1505 утечек конфиденциальной информации. Это на 7,8% больше, чем в 2014 году.

Рисунок 1 – Динамика количества утечек за 2007-2015гг.

Если перестроить распределение умышленных утечек в зависимости от вектора атаки, мы получим наглядное представление о «привлекательности» конкретной отрасли для внешнего и внутреннего злоумышленника.

Таблица 1 – Распределение утечек по отраслям

Отрасли	Доля утечек по вине внутреннего злоумышленника	Доля утечек по вине внешнего злоумышленника
Высокие технологии	9,5	57,4
Промышленность и транспорт	6,2	52,4
Торговля	5,9	44,4
Образовательные учреждения	5	32,3
Банки и финансы	12	25,6
Госорганы и силовые органы	7,3	19,8
Медицина	19,4	14,1
Муниципальные учреждения	6,9	2

Зарегистрировано 484 (32,2%) утечки информации, причиной которых стал внешний злоумышленник. В 984 (65,4%) случаях утечка информации произошла по вине или неосторожности внутреннего нарушителя.

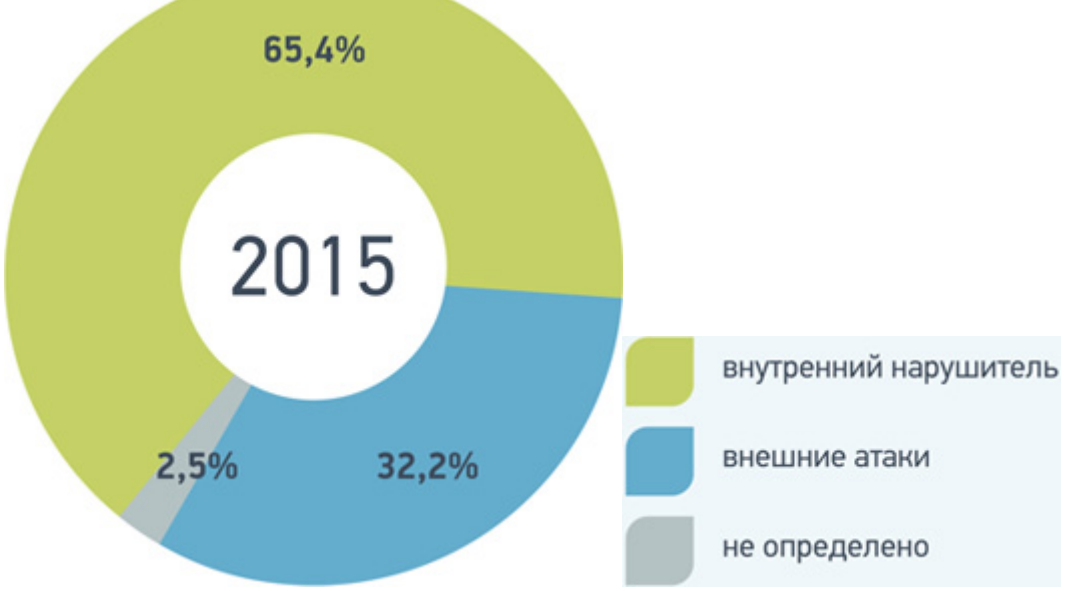

Рисунок 2 – Доля внутренних и внешних нарушителей

В 2015 году в 51,2% случаев виновниками утечек информации были настоящие или бывшие сотрудники – 48,9% и 2,3%соответственно. Более чем в 1% случаев зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов). Доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, выросла на 3,5 п. п., составив 7,6% (таблица 2).

Таблица 2 – Виновники утечек

Виновники утечек	**Доля утечек (%)**
Сотрудник	48,9
Внешний злоумышленник	32,2
Подрядчик	7,6
Бывший сотрудник	2,3

Системный администратор	1,4
Руководитель	1,1

Рисунок 3 – Доля утечек и виновники

Для 6,5% виновника утечки установить не удалось.

За 2015 год зафиксировано 21 «мега-утечка» данных (компрометация данных объемом свыше 10 млн. записей).

На «мега-утечки» приходится 814,5 млн. записей, скомпроментированных в результате утечек в 2015 году (84,3% от совокупного объема скомпрометированных данных).

Рисунок 4 – Виды утечек

7,7% инцидентов классифицированы как нарушения, сопряженные с получением несанкционированного доступа к информации (превышение прав доступа, манипуляции с информацией, которая не нужна сотруднику для исполнения служебных обязанностей).

Рисунок 5 – Распределение по характеру инцидентов

В 2015 году сократилась доля утечек по таким каналам, как «потеря оборудования» (на 8,3 п. п.), «электронная почта» (на 1,2 п. п.), «бумажные документы» (на 3,7 п. п.). Доли утечек через съемные носители, мобильные устройства текстовые и видеосообщения остались на уровне 2014 года. Доля «сетевого» канала выросла на 10,5 п. п.

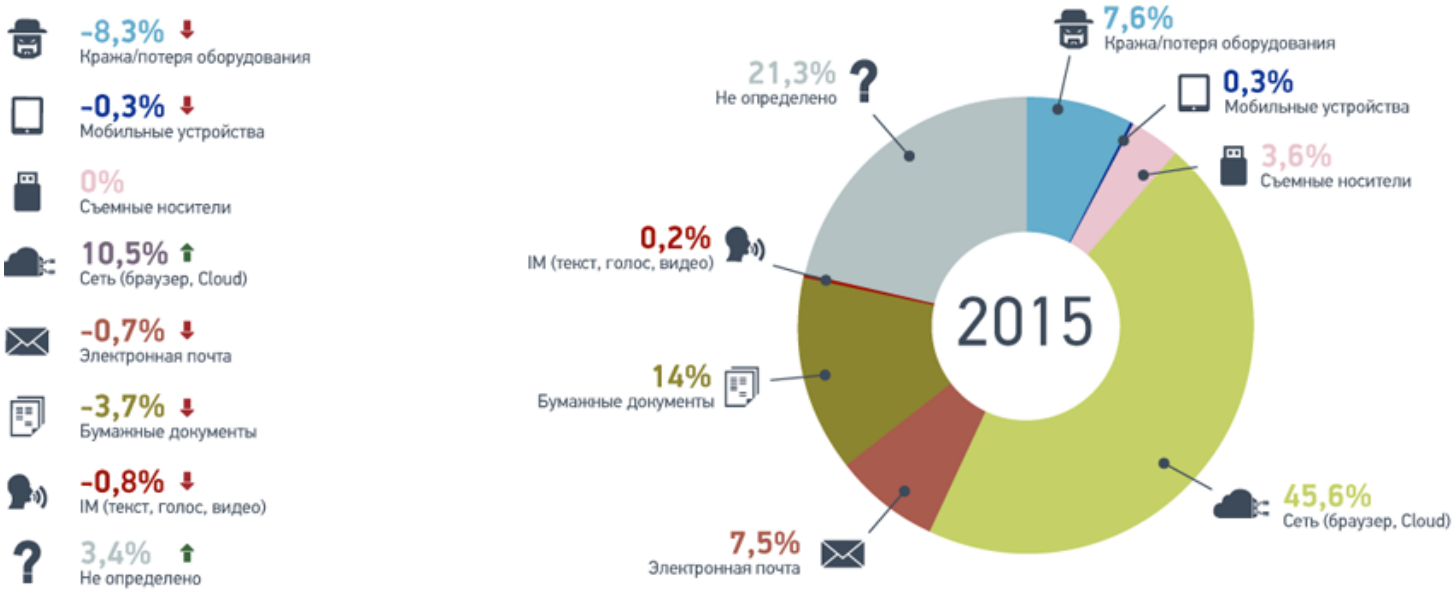

Рисунок 6 – Каналы утечек

По сравнению с данными 2014 года, распределение утечек по типу организации не претерпело существенных изменений.

Рисунок 7 – Распределение утечек по типу организации

Утечки по отраслям

Чаще всего утечки фиксировались в медицине **(20,2%)**, реже всего в муниципальных учреждениях **(<2%)**. По объему скомпрометированных записей пальма первенства безраздельно принадлежит компаниям высокотехнологичного сегмента (речь идет о крупных интернет-сервисах, торговых онлайн-площадках и пр.). На долю этих компаний приходится почти треть **(29,2%)** от всего объема скомпрометированных данных. Заметна доля образовательных учреждений – **20,2%.**

Рисунок 8 – Распределение утечек по отраслям

Наиболее уязвимыми отраслями оказались: сегмент высоких технологий, торговля, транспорт

Наибольший объем скомпрометированных данных (без учета «мега-утечек») пришелся на высокотехнологичные компании и организации в сфере образования. Данные торговых, транспортных, высокотехнологичных компаний чаще всего атакуют извне. В банках, страховании, медицине компрометация ПДн связана, как правило, с действиями внутренних злоумышленников. Средний бизнес подвержен

утечкам персональных данных в большей степени, чем крупные компании.

Утечки по странам

В распределении утечек по регионам в 2015 году США традиционно заняли первую позицию по количеству утечек (**859** или **57%** от всех произошедших). Россия оказалась на уже привычном втором месте (**118** утечек), опередив Великобританию всего на **6 инцидентов**.

Россия заняла второе место – 118 утечек.

2.2 Методы борьбы с угрозами

Под мерой защиты информации будем понимать действие или совокупность действий (в т.ч. применение средств) для осуществления защиты информации [8, с.56].

Под средством защиты информации будем понимать техническое, криптографическое, программное или другое средство, предназначенное для защиты информации, средства в которых они реализованы, а также средства контроля эффективности защиты информации.

Мероприятие по защите информации — совокупность действий по разработке и практическому применению мер и средств защиты информации. Общая классификация мер и средств защиты информации представлена на рис.9.

Рисунок 9 – Общая классификация мер и средств защиты информации [11, с.56]

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Благодаря организационной защите [8, с.87]:

- обеспечивается организация охраны, режима, работа с документами, с кадрами;
- используются технические средства безопасности и информационно-аналитическая деятельность с целью выявления внешних и внутренних угроз коммерческой деятельности.

Организационные меры защиты должны быть прописаны в документах, определяющих порядок обеспечения информационной безопасности в компании. Основным таким документом является политика информационной безопасности.

Под инженерно-технической защитой понимается совокупность технических средств, специальных органов и мероприятий по использованию технических средства с целью защиты конфиденциальной информации.
Выделяются следующие группы средств инженерно-технической защиты по функциональному назначению [11, с.29]:

Физические средства;

Аппаратные средства;

Программные средства;

Криптографические средства.

Физические средства включают различные сооружения и средства, которые препятствуют физическому доступу (или проникновению) нарушителей на объекты защиты и к материальным носителям конфиденциальной информации и осуществляют защиту материальных средств, персонала, информации и финансов от противоправных воздействий. Физическими средствами являются механические, электронно-оптические, электромеханические электронные, радио- и радиотехнические и другие устройства для запрета несанкционированного доступа, проноса (выноса) материалов и средств и других возможных видов преступных действий.

Меры контроля физического доступа к элементам ИС сводятся к применению средств и систем контроля физического доступа, которые создают препятствия для нарушителей на путях к защищаемым данным, например, на территорию, на которой располагаются объекты информатизации, в помещения с аппаратурой, носителями данных и т.п., и обеспечивают контроль доступа.

Система обнаружения вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Internet. Соответствующий английский термин – Intrusion Detection System (IDS).

Общая классификация СОВ представлена на рис.10.

Рисунок 10 – Классификация систем обнаружения вторжений

Программные средства охватывают специальные программные комплексы, программы и системы защиты информации в ИС различного назначения и средствах обработки (накопления, сбора, хранения, передачи и обработки) данных.

Криптографические средства – это специальные алгоритмические и математические средства защиты информации, которая передается по сетям и системам связи, хранится и обрабатывается на ПК с применением различных методов шифрования.

В качестве **методов криптографической защиты** применяются протоколы TLS и SSH, также применяются VPN [13, с.111].

Технология виртуальных частных сетей (Virtual Private Network) — это технология эмуляции соединения «точка-точка» через сеть общего пользования. При этом между хостом пользователя и провайдером организуется так называемый туннель, по которому пакеты исходящей от пользователя информации достигают провайдера [12, с.59].

Виртуальные частные сети применяются для создания безопасных и надежных каналов, связывающих локальные сети и обеспечивающих доступ к ним пользователей, постоянно меняющих свое географическое местоположение. В основе этих сетей лежит использование открытой и общедоступной сети, такой как Internet.

Для защиты от наиболее распространенных компьютерных преступлений используются системы обнаружения вторжений и антивирусные комплексы.

Заключение

До недавнего времени к числу наиболее распространённых причин нарушения стабильной деятельности фирм и предприятий относили стихийные бедствия, пожары и хищения материальных ценностей.

С появлением новых форм собственности и рыночных отношений, развитием все новых информационных технологий все чаще приходится сталкиваться с проявлениями несанкционированного доступа к информации, попытками хищения, терроризма, вандализма и другими преступлениями, направленными как против личности, чаще всего руководителя и владельцев, так и против всего объекта в целом.

Таким образом, одним из главных условий стабильной работы предприятия становится обеспечение безопасности его деятельности, что приобретает на сегодня все более сложный, разносторонний, комплексный характер и требует определённых системных мер защиты. Чтобы избежать вышеперечисленных угроз, необходим комплексный подход к системе безопасности, который включает в себя защиту всех систем.

В работе был проведен обзор состояния угроз в 2015 году. Были получены следующие выводы.

Наиболее весомый вклад в увеличение объема скомпрометированных данных принадлежит внешним атакам.

Уже сейчас на долю внешних атак приходится до двух третей от совокупного объема скомпрометированных ПДн, чуть менее 1 млрд записей.

Растет «квалификация» внутреннего нарушителя.

Самыми «привлекательными» для злоумышленников уязвимыми отраслями оказались сегмент высоких технологий, торговля, транспорт.

Наибольший объем скомпрометированных данных (без учета «мега-утечек») пришелся на высокотехнологичные компании и организации в сфере образования.

Список использованной литературы

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» / "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3451
2. Федеральный закон Российской Федерации от 26 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» / "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3448
3. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012г. № 1119 / "Собрание законодательства РФ", 05.11.2012, N 45, ст. 6257
4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. URL: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005
5. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. URL: http://docs.cntd.ru/document/gost-r-51275-2006
6. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 2-е изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. – 392 с.
7. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К. Баранова, А.В. Бабаш – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 – 120 с.
8. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. – 2-е изд., испр. и доп. – М.: Форум: НИЦ ИНФРА-М, 2015. – 352 с.
9. Базовые и прикладные информационные технологии: Учебник / В.А. Гвоздева. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2015. – 384 с.
10. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 2-е изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. – 392 с.
11. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – 2-е изд., доп. – М.: Форум: НИЦ ИНФРА-М, 2015. – 240 с.
12. Информационная система предприятия: Учебное пособие / Л.А. Вдовенко – 2 изд., перераб. и доп. – М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. – 304 с.
13. Информационные технологии в профессиональной деятельности: Учебное пособие / Е.Л. Федотова. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. – 368 с.