Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

ОРГАНИЗАЦИЯ ЗАЩИТЫ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ И КОММЕРЧЕСКОЙ ТАЙНЫ

сборник учебно-методических материалов
для специальности 38.05.01 - Экономическая безопасность

Благовещенск 2017

Печатается по решению

редакционно-издательского совета

экономического факультета

Амурского государственного

университета

Составитель: Бальцежак М.С.

Организация защиты экономической информации и коммерческой тайны: сборник учебно-методических материалов для специальности 38.05.01 Экономическая безопасность. – Благовещенск: Амурский гос. ун-т, 2017.

СОДЕРЖАНИЕ

1. Краткое изложение лекционного материала 4
2. Методические рекомендации (указания) к практическим занятиям 41
3. Методические указания для самостоятельной работы студентов 43

Краткое изложение лекционного материала

Лекция – одна из базовых форм обучения обучающихся. Углубляясь в значение термина, можно сказать, что лекцией следует называть такой способ изложения информации, который имеет стройную логическую структуру, выстроен с позиций системности, а также глубоко и ясно раскрывает предмет.

В зависимости от задач, назначения и стиля проведения различают несколько основных видов лекций: вводная, информационная, обзорная, проблемная, визуализационная, бинарная ,конференция, консультация. Лекция, особенно проблемного характера, дополняет учебники и учебные пособия. Она оказывает существенное эмоциональное влияние на обучающихся, будит мысль, формирует интерес и желание глубоко разобраться в освещаемых лектором проблемах.

Тема 1. Основы информационной безопасности и защиты информации

План:

1. Информация и информационная безопасность.
2. Основные составляющие информационной безопасности.
3. Объекты защиты.
4. Категории и носители информации.
5. Средства защиты информации.

1. ***Информация*** (лат. in ormatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины 20-го века ***информация*** является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом;
- сигналы в животном и растительном мире;
- признаки, передаваемые от клетки к клетке, от организма к организму;
- и т.д.

Другими словами, информация носит фундаментальный и универсальный характер, являясь многозначным понятием. Эту мысль можно подкрепить словами Н. Винера (отца кибернетики): «Информация есть информация, а не материя и не энергия».

Согласно традиционной философской точке зрения, информация существует независимо от человека и является свойством материи. В рамках рассматриваемой дисциплины, под ***информацией*** (в узком смысле) мы будем понимать сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах[1].

Опираясь на это определение информации, рассмотрим понятия информационной безопасности и защиты информации.

В Доктрине информационной безопасности Российской Федерации под термином ***информационная безопасность*** понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В более узком смысле, под ***информационной безопасностью*** понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Защита информации – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

Важно отметить, что информационная безопасность – это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который

должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.

Рассмотрим более подробно составляющие этих определений.

Под ***субъектами информационных отношений*** понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

К ***поддерживающей инфраструктуре*** относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Ущерб может быть ***приемлемым*** *или* ***неприемлемым***. Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации.

2. Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие составляющие:

обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих информационной безопасности включают защиту от несанкционированного доступа (НСД) к информации, под которым понимают доступ к информации, нарушающий правила разграничения доступа с использование штатных средств. В то же время обеспечение конфиденциальности как раз и подразумевает защиту от НСД.

Определения основных составляющих информационной безопасности:

Доступность информации – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность информации – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций[4])). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

Конфиденциальность информации – свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожале-

нию, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность.

3. Основными ***объектами защиты*** при обеспечении информационной безопасности являются:

- все виды информационных ресурсов.

Информационные ресурсы (документированная информация) - информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

- права граждан, юридических лиц и государства на получение, распространение и использование информации;

- система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.);

- система формирования общественного сознания (СМИ, социальные институты и т.д.).

4. Неотъемлемой частью любой информационной системы является информация. По характеру ограничений (реализации) конституционных прав и свобод в информационной сфере выделяют четыре основных ***вида правовой*** (регламентированной законами) ***информации***:

- информация с ограниченным доступом;

- информация без права ограничения;

- иная общедоступная информация (например, за деньги);

- «вредная» информация (информация, не подлежащая распространению как недостоверная, ложная и т.п.).

Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.

К ***государственной тайне*** относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Владельцем государственной тайны является само государство. Требования по защите этой информации и контроль за их соблюдением регламентируются Законом РФ «О государственной тайне». В нем законодательно установлен Перечень сведений, сопоставляющих государственную тайну, и круг сведений, не подлежащих к отнесению к ней. Предусмотрена судебная защита прав граждан в связи с необоснованным засекречиванием. Определены органы защиты государственной тайны:

- межведомственная комиссия по защите государственной тайны;

- федеральные органы исполнительной власти, уполномоченные в области:

- обеспечения безопасности - Федеральная служба по техническому и экспортному контролю (ФСТЭК);

- обороны – Министерство обороны;

- внешней разведки – Федеральная служба безопасности (ФСБ обеспечивает, в т.ч. криптографическую защиту);

- противодействия техническим разведкам и технической защиты информации – ФСТЭК;

- другие органы.

Конфиденциальная информация – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности. Этой информацией владеют различные учреждения, организации и отдельные индивидуумы. В Указе Президента РФ

«Перечень сведений конфиденциального характера» конфиденциальная информация разбита на шесть видов:

- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца по официальной публикации информации о них;
- персональные данные.

Под ***персональными данными*** понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Некоторая часть персональных данных может не иметь режима защиты, являясь общеизвестными (например, фамилия, имя и отчество). В Законе РФ «О персональных данных» выделены следующие ***права субъектов персональных данных*** (кроме некоторых категорий граждан: владеющих государственной тайной, осужденных и т.д.):

- информационное самоопределение;
- доступ к своим персональным данным;
- внесение изменений в свои персональные данные;
- блокирование персональных данных;
- обжалование неправомерных действий в отношении персональных данных;
- возмещение ущерба.

Государственные органы и организации, органы местного самоуправления имеют право на работу с персональными данными в пределах своей компетенции, установленной действующим законодательством, или на основании лицензии. В последнем случае с ними могут работать также негосударственные юридические и физические лица.

Основными ***носителями информации*** являются:

- открытая печать (газеты, журналы, отчеты, реклама и т.д.);
- люди;
- средства связи (радио, телевидение, телефон, пейджер и т.д.);
- документы (официальные, деловые, личные и т.д.);
- электронные, магнитные и другие носители, пригодные для автоматической обработки данных.

5. Принято различать следующие средства защиты:

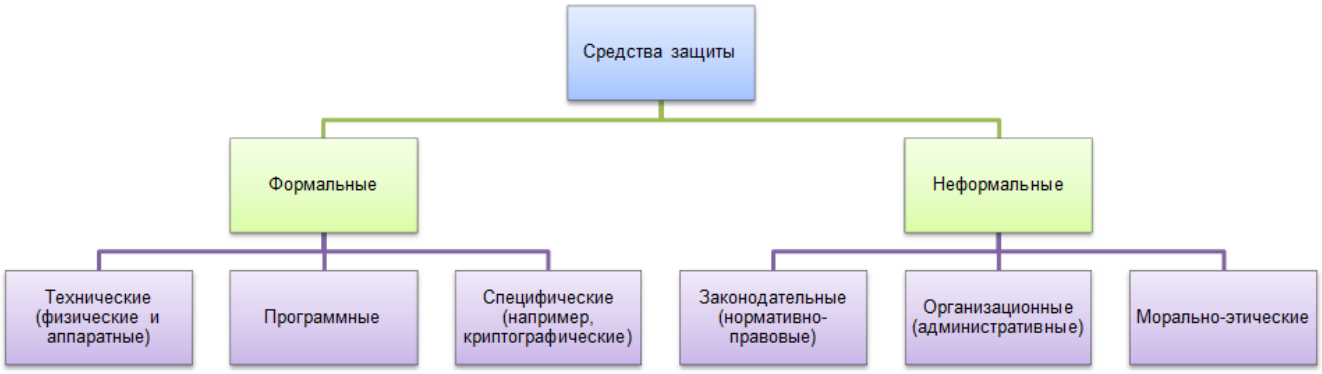


Рисунок 1. - Классификация средств защиты

Формальные средства защиты – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

Аппаратные средства - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

К ***специфическим средствам*** защиты информации относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

Неформальные средства защиты – регламентируют деятельность человека.

Законодательные средства – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений.

Организационные средства - организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем).

Морально-этические средства - сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета. Наиболее показательные пример – кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

Тема 2. Виды и особенности угроз информационной безопасности

План:

1. Угрозы безопасности информационных ресурсов.
2. Система защиты конфиденциальной информации
3. Промышленный и экономический шпионаж, его сущность, история и сфера распространения.
4. Меры по обеспечению информационной безопасности

1. ***Угроза информационной безопасности*** — это совокупность условий и факторов, создающих опасность не обеспечения решения хотя бы одной из задач информационной безопасности. Угроза информационной безопасности — это возможность того, что произойдёт некоторое событие или последовательность событий, при которых применяемые на данный момент решения задач информационной безопасности не сработают.

Окно опасности — это время, в течении которого существует угроза информационной безопасности. Как правило, появлением окна опасности считают момент обнаружения угрозы, а закрытием окна — момент ликвидации угрозы.

Существует несколько различных подходов к классификации, соответственно и несколько классификаций.

Типы угроз по аспекту (задаче) информационной безопасности, на который они направлены:

1) угрозы конфиденциальности — состоит в том, что к информации получает доступ тот, кто не должен этого доступа иметь, в таком случае говорят об «утечке информации» (пример: к информации о ваших банковских счетах получил доступ допустим ваш сосед); 2) угрозы целостности — состоит в неправомерном изменении данных (например дети вашего соседа изменили дан-

ные вашего профиля в социальной сети); 3) угрозы доступности — состоит в том, что круг лиц, который должен обладать доступом к информации, либо лишается этого доступа совсем, либо качество доступа значительно снижается (примерами реализаций таких угроз можно назвать DDOS-атаки на сайты — в этом случае, легальные пользователи либо не могут зайти на сайт, либо страницы загружаются на столько медленно, что нормальное использование сайта не возможно).

Вторая классификация — ***угрозы информационной безопасности по расположению источника угроз:*** 1) внешние — источники угроз находятся вне системы (например, природные катаклизмы); 2) внутренние — источники угроз находятся внутри системы (пример: сотрудник организации). Третья классификация — угрозы информационной безопасности по природе возникновения: 1) естественные (объективные) — угрозы, вызванные воздействием на систему объективных физических процессов (например, старение, износ и разрушение аппаратуры с течением времени) или природных явлений, не зависящих от воли человека; 2) искусственные (субъективные) — угрозы, вызванные преднамеренным или непреднамеренным воздействием на систему человека. Непреднамеренные или случайные угрозы — угрозы, вызванные ошибками программного обеспечения, персонала, сбои в работе техники и т. п.

Преднамеренные или умышленные угрозы — любые угрозы информационной безопасности, возникшие в результате преднамеренных и целенаправленных действий человека (злоумышленника). Именно преднамеренные угрозы являются основной проблемой информационной безопасности.

Источник угрозы информационной безопасности — это некто или нечто, могущее реализовать угрозу. В качестве источников угроз можно назвать людей, организации, природные явления и др. Люди и организации, как правило, преследуют следующие цели при попытках обойти систему обеспечения информационной безопасности: 1) ознакомление с защищаемой информацией; 2) изменение защищаемой информации; 3) уничтожение защищаемой информации. В каждом из этих случаев злоумышленник стремится получить выгоду или нанести ущерб.

Для автоматизированных информационных систем угрозы следует классифицировать прежде всего по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь:

— угрозы нарушения доступности (отказ в обслуживании), направленные на создание таких ситуаций, когда определенные действия либо блокируют доступ к некоторым ресурсам ИС, либо снижают ее работоспособность. Блокирование доступа к ресурсу может быть постоянным или временным;

— угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему.

— угрозы нарушения конфиденциальности, направленные на разглашение конфиденциальной или секретной информации.

С точки зрения безопасности распределенные системы характеризуются прежде всего наличием удаленных атак, поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие). И если активное воздействие на трафик может быть зафиксировано, то пассивное воздействие практически не поддается обнаружению. Но поскольку в ходе функционирования распределенных систем обмен служебной информацией между компонентами системы осуществляется тоже по открытым каналам передачи данных, то служебная информация становится таким же объектом атаки, как и данные пользователя.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными.

Существуют четыре основные категории ***сетевых атак***:

— атаки доступа;

— атаки модификации;
— атаки на отказ в обслуживании;
— комбинированные атаки.

Атака доступа – это попытка получения злоумышленником информации, для ознакомления с которой у него нет разрешения. Атака до-ступа направлена на нарушение конфиденциальности информации.

Атака модификации – это попытка неправомочного изменения информации. Такая атака возможна везде, где существует или передается информация; она направлена на нарушение целостности информации.

Атака на отказ в обслуживании (Denial-o -Service, DoS) отличается от атак других типов. Она не нацелена на получение доступа к корпоративной сети или на получение из этой сети какой-либо информации.

Комбинированные атаки заключаются в применении злоумышленником нескольких взаимно связанных действий для достижения своей цели

2. ***Обладатель информации*** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Шпионаж – передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности Российской Федерации.

Система защиты информации — рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. Главными требованиями к организации эффективного функционирования системы являются: персональная ответственность руководителей и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений и документов, подлежащих защите, регламентация порядка доступа персонала к конфиденциальным сведениям и документам, наличие специализированной службы безопасности, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности этой службы.

Собственники информационных ресурсов, в том числе государственные учреждения, организации и предприятия, самостоятельно определяют (за исключением информации, отнесенной к государственной тайне) необходимую степень защищенности ресурсов и тип системы, способы и средства защиты, исходя из ценности информации. Ценность информации и требуемая надежность ее защиты находятся в прямой зависимости.

Основной характеристикой системы является ее комплексность, т.е. наличие в ней обязательных элементов, охватывающих все направления защиты информации. Соотношение элементов и их содержания обеспечивают индивидуальность построения системы защиты информации конкретной фирмы и гарантируют неповторимость системы, трудность ее преодоления. Конкретную систему защиты можно представить в виде кирпичной стены, состоящей из множества разнообразных элементов (кирпичиков). Элементами системы являются:

— правовой,
— организационный,
— инженерно-технический,
— программно-аппаратный
— криптографический

3. Одним из наиболее опасных для нормального осуществления предпринимательства видов незаконной деятельности является коммерческий шпионаж. Коммерческий шпионаж — это дейст-

вия лиц, направленные на незаконное получение коммерческой информации, находящейся под защитой. Коммерческий шпионаж включает промышленный, производственный, научно-технический шпионаж и т.д. Объектом коммерческого шпионажа является информация, составляющая коммерческую тайну. Утечка этой информации может привести к реальным потерям для фирмы либо к упущенной выгоде или к обоим последствиям сразу. Чаще всего коммерческий шпионаж осуществляется: конкурентами;– криминальными структурами;– лицами, стремящимися получить доход от перепродажи полученных– незаконным путем сведений. В условиях острой конкурентной борьбы каждая фирма, действующая на рынке, неизбежно сталкивается с необходимостью решения двух проблем. Первая проблема связана с получением информации о деятельности конкурентов, причем как можно более полной, точной и своевременной. Без

наличия такой информации невозможно разрабатывать производственную, научно-техническую, финансовую, рыночную стратегии и тактику поведения фирмы. Вторая проблема — защита конфиденциальной информации. Как сама фирма стремится узнать секреты других, так и ее конкуренты делают то же самое. Следовательно, каждая фирма может являться одновременно как объектом, так и субъектом коммерческого шпионажа, или, если использовать более «мягкий» термин — экономической разведки. 2. Субъекты и объекты коммерческого шпионажа Законодательство предусматривает, что если в процессе хищения секретной информации предприятию, учреждению или сотрудникам причиняется ущерб, то уголовному наказанию виновное лицо повергается именно за последнее деяние, а не за сам факт хищения ценнейших сведений. Остановимся на признаках, характеризующих коммерческий шпионаж. К ним относятся: субъект (кто может заниматься данным видом деятельности);– объект (на что посягает промышленный и иной шпионаж);– способ, средство (действия, с помощью которых осуществляется овладение– закрытыми сведениями); адресат (кто выступает заказчиком).– Субъектом коммерческого шпионажа в развитых странах все чаще становятся не сами фирмы-конкуренты, а специализированные коммерческие организации, основной целью деятельности которых как раз и является изъятие или защита конфиденциальной информации. Объектом преступных посягательств являются персонал фирмы), документы, технические средства. Непосредственным носителем информации могут быть бумажные документы, планы, отчеты, финансовые документы, чертежи, техническая документация, диски и другие электронные носители информации.

Способы коммерческого шпионажа Способы коммерческого шпионажа, как правило, весьма разнообразны, и во многом такая преступная деятельность осуществляется на профессиональной основе с использованием традиционного набора шпионских методов и средств получения сведений, составляющих коммерческую или банковскую тайну. Чаще всего при совершении коммерческого шпионажа применяются следующие способы: - подкуп работников организации, имеющих доступ к документам, содержащим коммерческую или банковскую тайну (получение вознаграждения или взятки лицом, обладающим такой информацией; «переманивание» сотрудника организации с целью использования его знаний о конфиденциальных источниках информации); - склонение к разглашению коммерческой или банковской тайны сотрудников организации, имеющих доступ к конфиденциальным сведениям, а также лиц, сменивших прежнее место работы, или пенсионеров, имевших доступ к закрытой информации (с использованием подкупа, различных угроз, принуждения, вербовки и т. д.); - внедрение агентов на должности, позволяющие получить непосредственный доступ к сведениям и документам, содержащим коммерческую или банковскую тайну, либо скрытно собирать информацию в процессе служебной (производственной) деятельности; - использование источников информации в финансовых и налоговых органах, государственных структурах, правоохранительных органах с целью получения закрытой (конфиденциальной) информации субъекта хозяйствования; - подкуп посредников в торговых переговорах; - проведение разведывательного опроса (замаскированное выведывание сведений у осведомленных лиц, которые разглашают конфиденциальную информацию, не осознавая этого, с использованием специальных анкет и вопросников, рассылаемых организациями по почте, факсу и другими способами); - перехват информации, циркулирующей в технических средствах и помещениях (служебных, жилых, производственных); - прямое завладение документами, содержащими коммерческую или банковскую тайну (копирование такой информации, ее кража, подмена другими сведениями, по-

хищение различных изделий, микросхем, агрегатов, технических документов, ноутбуков с конфиденциальной информацией и т. д.); - собирание сведений, составляющих коммерческую или банковскую тайну, должностными лицами тех органов, которые имеют право такие сведения получать с нарушением порядка их получения, без надлежащих оснований, прямого похищения информации; - использование специальных технических средств, предназначенных для негласного получения информации (акустический контроль помещения, автомобиля, непосредственного поведения человека и его переговоров; контроль и прослушивание телефонных переговоров); - несанкционированный доступ к сведениям, содержащимся в средствах вычислительной техники и электронных банках данных (электромагнитный перехват; несанкционированный доступ в компьютерную сеть; непосредственный перехват компьютерной информации, который осуществляется через внешние коммуникационные каналы системы либо путем непосредственного подключения.

4. Меры по обеспечению информационной безопасности делятся на следующие группы: 1) нормативно-правовые и научные; 2) административные; 3) организационно-технические; 4) программно-технические меры.

Нормативно-правовые и научные меры. К данной группе мер относятся законодательные и иные нормативно-правовые акты разного уровня, определяющие понятия, определения, требования, разрешения, запреты и ответственность за их соблюдение, действующие в области информационной безопасности и зафиксированные юридически. К этой же группе относятся стандарты информационной безопасности: стандарты предприятий, ГОСТы, международные стандарты и стандарты других стран. А так же различные научные изыскания в области информационной безопасности и защиты информации.

Административные меры. К этой группе мер относятся создание и функционирование различных подразделений, занимающихся обеспечением информационной безопасности. Это может быть и один специалист по информационной безопасности, занимающийся защитой информации на небольшом предприятии, и полномасштабные государственные структуры, решающие похожие задачи только уже на другом уровне, например Роскомнадзор и другие подразделения, занимающиеся преступлениями в сфере информационных технологий**.**

Организационно-технологические меры Эта группа мер представлена решениями о том, как должны функционировать элементы защищаемой системы и какие работы должны производиться в системе постоянно, периодически, а какие — в случае возникновения той или иной ситуации. Данные решения оформляются и закрепляются в виде специальных документов. Одним основополагающих документов такого типа является политика безопасности. Система здесь понимается в широком смысле: программная часть, аппаратная часть, персонал и обеспечивающие подсистемы.

Политика безопасности — это совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту, использование и распределение ценной информации.

Программно-технические меры К этой группе мер относится использование специальных программных и аппаратных средств, применяемых для решения задач информационной безопасности. Примерами таких средств являются антивирусы, межсетевые экраны, генераторы паролей, программы для шифрования и дешифровки, разграничения доступа, электронные ключи, биометрические сканеры и т. п.

Конкретные меры и их применение для решения задач информационной безопасности:

1) резервирование и дублирование мощностей, использование систем бесперебойного питания, создание резервных копий информации применяются для обеспечения доступности информации; 2) электронная цифровая подпись (ЭЦП), шифрование, хеширование, помехоустойчивое кодирование (ведь как отмечалось, искажения информации мо-гут происходить в результате случайный сбоев в работе техники или в результате воздействия внешней среды на канал связи), стеганографическое скрытие, резервирование, дублирование, резервное копирование, разграничение прав доступа, журнализация — эти меры позволяют обеспечить целостность информации; 3) шифрование, стеганографическое скрытие, безвозвратное удаление, разграничение прав доступа,

контроль потоков информации, журнализация — эти меры позволяют обеспечить конфиденциальность данных; 4) электронная цифровая подпись и журнализация — на данный момент одни из основных средств для решения задачи обеспечения неотказуемости; 5) журнализация — основное средство обеспечения подотчетности.

Тема 3. Правовое регулирование открытых информационных ресурсов и ресурсов ограниченного доступа

План:

1. Защита информации институтом интеллектуальной собственности
2. Характеристика норм патентного права
3. Характеристика норм авторского права и смежных прав
4. Страхование ценной информации

1. Интеллектуальная собственность включает в себя:

• литературные, художественные и научные произведения;
• исполнительскую деятельность артистов, звукозаписей, радио- и телевизионные передачи;
• изобретения во всех областях человеческой деятельности;
• научные открытия;
• промышленные образцы;
• полезные модели;
• товарные знаки и фирменные наименования.

Результатами интеллектуальной деятельности являются:

• стихи, проза, научные статьи;
• программы для ЭВМ и базы данных;
• исполнения и фонограммы;
• сообщения в эфир или по кабелю, радио- или телепередачи;
• изобретения, полезные модели и промышленные образцы;
• секреты производства (ноу-хау).

Интеллектуальное право является подотраслью гражданского права. Право интеллектуальной собственности можно определить как систему правовых норм, регулирующих имущественные и личные неимущественные отношения, возникающие в связи с созданием и использованием результатов интеллектуальной деятельности и средств индивидуализации. Задачами права интеллектуальной собственности являются:

• стимулирование деятельности по созданию объектов интеллектуальной собственности;
• создание условий для использования результатов интеллектуальной деятельности в интересах общества;
• обеспечение условий для добросовестной конкуренции

Исключительное право означает право использовать результат интеллектуальной деятельности любым способом, не противоречащим закону. Исключительное право даёт возможность правообладателю разрешать или запрещать другим лицам использование результатов интеллектуальной деятельности. Исключительное право является абсолютным и должно соблюдаться любыми субъектами. Первоначальным субъектом исключительного права является автор (соавторы), творческим трудом которого создан результат интеллектуальной деятельности.

Распоряжение исключительным правом возможно двумя способами: путём заключения договора об отчуждении исключительного права и путём предоставления права использования объекта интеллектуальной собственности в установленных договором пределах. По договору об отчуждении исключительного права одна сторона (правообладатель) передаёт принадлежащее ей исключительное право на результат интеллектуальной деятельности в полном объёме другой стороне (приобретателю). Договоры о распоряжении исключительным правом заключаются в письменной форме и подлежат государственной регистрации.

За ***нарушение интеллектуальных прав*** законом предусмотрена уголовная, административная, гражданско-правовая и дисциплинарная ответственность. К мерам гражданско-правовой от-

ветственности относятся: • возмещение убытков; • выплата компенсаций; • компенсация морального вреда; • ликвидация юридического лица за неоднократные или грубые нарушения исключительных прав. Размер компенсации определяется судом в пределах, установленных Гражданским Кодексом РФ, в зависимости от характера нарушения и иных обстоятельств дела с учётом требований разумности и справедливости.

2. ***Авторское право —*** совокупность правовых норм, регламентирующих отношения, возникающие в связи с созданием и использованием произведений литературы, искусства и науки. Принципы авторского права:

- свобода творчества;
- сочетание личных интересов автора с интересами общества;
- неотчуждаемость личных, неимущественных прав автора;
- свобода авторского договора.•

В зависимости от вида произведений различают следующие объекты авторского права:

1) литературные произведения;
2) музыкально-драматические и сценарные произведения;
3) хореографические произведения и пантомимы;
4) произведения живописи, скульптуры и дизайна;
5) произведения декоративно-прикладного искусства;
6) произведения архитектуры, строительства и садово-паркового искусства;
7) фотографические произведения;
8) географические и геологические карты.

Объекты авторского права подразделяют на: оригинальные и производные, простые и составные, обнародованные и необнародованные. В производных произведениях есть элементы заимствования или переработки. Составные произведения по подбору и расположению материала являются результатом творческого труда. Не являются объектами авторского права:

1) официальные документы;
2) государственная символика и знаки;
3) произведения народного творчества;
4) сообщения о событиях и фактах, имеющих информационный характер.

Неимущественные права:

право признаваться автором произведения;
право на имя (использование произведения под собственным именем или псевдонимом);
право на обнародование;
право на защиту произведения от искажения или иного посягательства,
способного нанести ущерб чести и достоинству автора;
личные неимущественные права автора принадлежат ему независимо от его имущественных прав.

Имущественные права: право на воспроизведение (изготовление одного или более экземпляров произведения в любой материальной форме);
право на распространение;
право на импорт;
право на публичный показ;
право на публичное исполнение;
право на передачу в эфир или по кабелю; право на перевод и переработку.

Субъектами ***смежных прав*** являются исполнители, производители фонограмм, организаторы эфирного или кабельного вещания. Смежные права - производные от авторских, их обладатели обязаны соблюдать права авторов и пользоваться ими в рамках установленных законов. Для оповещения о смежных правах на исполнение и фонограммы используется знак охраны смежных прав, состоящий из трех элементов: символ, имя или наименование обладателя и год первого опубликования фонограммы. Содержание смежных прав, по аналогии с авторским правом, составляют имущественные и неимущественные права. Неимущественные права:

1) право на имя;

2) право на защиту исполнения или постановки от искажения или иного посягательства, способного нанести ущерб чести или достоинству исполнителя.

Имущественные права:

1) передавать в эфир или по кабелю;

2) записывать ранее не записанные исполнения или постановку;

3) воспроизводить запись исполнения или постановки.

За ***нарушение авторского и смежного права*** наступает гражданская, уголовная, административная ответственность. Контрафактными являются экземпляры произведения или фонограммы, изготовление и распространение которые ведёт к нарушению авторских и смежных прав. Контрафактными являются также экземпляры охраняемых в РФ произведений и фонограмм, импортируемые без согласия обладателей авторских и смежных прав в РФ. Обладатели исключительных авторских и смежных прав вправе потребовать от нарушителя:

1. Признания прав.

2. Восстановления положения, существовавшего до нарушения права.

3. Возмещения убытков, включая упущенную выгоду.

Контрафактные экземпляры произведений подлежат конфискации и уничтожению.

3. ***Патентное право*** возникает в связи с созданием правовой охраны и использованием изобретений, полезных моделей и промышленных образцов (объекты промышленной собственности). Права на изобретения, полезную модель, промышленный образец охраняет закон и подтверждает патент, который удостоверяет приоритет авторства изобретения, промышленного образца и исключительное право на их использование. Патент на изобретение действует в течение 20 лет с момента поступления заявки в патентное ведомство. Патент на полезную модель - 10 лет. Патент на промышленный образец - 15 лет. Отсчёт идёт с даты поступления заявки в патентное ведомство. Правовая охрана не предоставляется изобретениям, полезным моделям и промышленным образцам, признанным государством секретными.

Изобретение является промышленно применимым, если его можно использовать в промышленности и других отраслях деятельности.

Объектами изобретения являются:

• устройства;

• способы;

• вещества;

• штаммы микроорганизмов, культуры клеток растений и животных.

Не признаются патентоспособными изобретениями:

• научные теории и математические методы;

• методы организации и управления хозяйством;

• методы выполнения умственных операций;

• алгоритмы программ для ЭВМ;

• схемы планировки зданий, сооружений, территорий;

• топологии интегральных микросхем;

• сорта растений и породы животных;

• решения, противоречащие общественным интересам, принципам

Полезной модели предоставляется правовая охрана (малый патент), если она является новой и промышленно применимой. Полезная модель является новой, если совокупность её существенных признаков неизвестна на уровне техники. Уровень техники подразумевает запатентованные в РФ изобретения и полезные модели. В качестве полезных моделей не охраняются:

• способы;

• вещества;

• штаммы микроорганизмов;

• культуры клеток, растений и животных, а также всё то, что не признаётся изобретениями.

Объектом полезной модели является только устройство.

Автором изобретения, полезной модели, промышленного образца признаётся только физическое лицо, творческим трудом которого они были созданы. Не признаются авторами физические лица, не внесшие личного творческого вклада в создание объекта промышленной собственности, оказавшие автору только техническую, организационную или материальную помощь. Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Патент выдаётся авторам – физическим или юридическим лицам, которые указаны в заявке на выдачу патента. Право на получение патента на созданное работником во время выполнения служебных обязанностей изобретение принадлежит работодателю, при этом автор имеет право на вознаграждение, соразмерное выгоде, полученной работодателем

Получение патента. Заявка на выдачу патента подаётся автором или работодателем в патентное ведомство РФ. Заявка на изобретение должна содержать:

1. Заявление о подаче патента с местом жительства.
2. Описание изобретения.
3. Формулу изобретения, выражающую его сущность и полностью основанную на описании.
4. Чертежи или схемы, необходимые для понимания сущности изобретения.
5. Реферат (краткое содержание сути изобретения).

Заявка на полезную модель должна содержать:

1. Заявление о выдаче патента с указанием авторов и их места жительства.
2. Описание полезной модели.
3. Формулу полезной модели.
4. Чертежи.
5. Реферат.

Заявка на промышленный образец должна содержать:

1. Заявление.
2. Комплект фотографий, отображающих изделие, дающий полное детальное представление о внешнем виде изделия.
3. Эргономическую схему и чертежи.
4. Описание промышленного образца, включающее перечень его существенных признаков.

Ко всем заявкам на объект промышленной собственности обязательно прилагается документ об уплате государственной пошлины.

4. Согласно Закону РФ "Об организации страхового дела в Российской Федерации", объектом страхования могут быть не противоречащие законодательству имущественные интересы, связанные с владением, пользованием, распоряжением имуществом, а также связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу (страхование ответственности). Таким образом, на практике объектами страхования могут быть:

−информационные ресурсы (в любом их виде: базы данных, библиотеки электронных документов и т.п.);

−программное обеспечение (как уже используемые программные собственные и покупные продукты, так и находящиеся в разработке);

−аппаратное обеспечение информационных систем (сетевое оборудование, серверы, рабочие станции, телекоммуникационное оборудование, периферия, источники бесперебойного питания и т.п.);

−финансовые активы (денежные средства, бездокументарные ценные бумаги) в электронной форме (в том числе средства на счетах, управляемых при помощи систем "клиент-банк").

Процедура страхования (жизненный цикл договора страхования) включает в себя несколько основных этапов (рисунок).

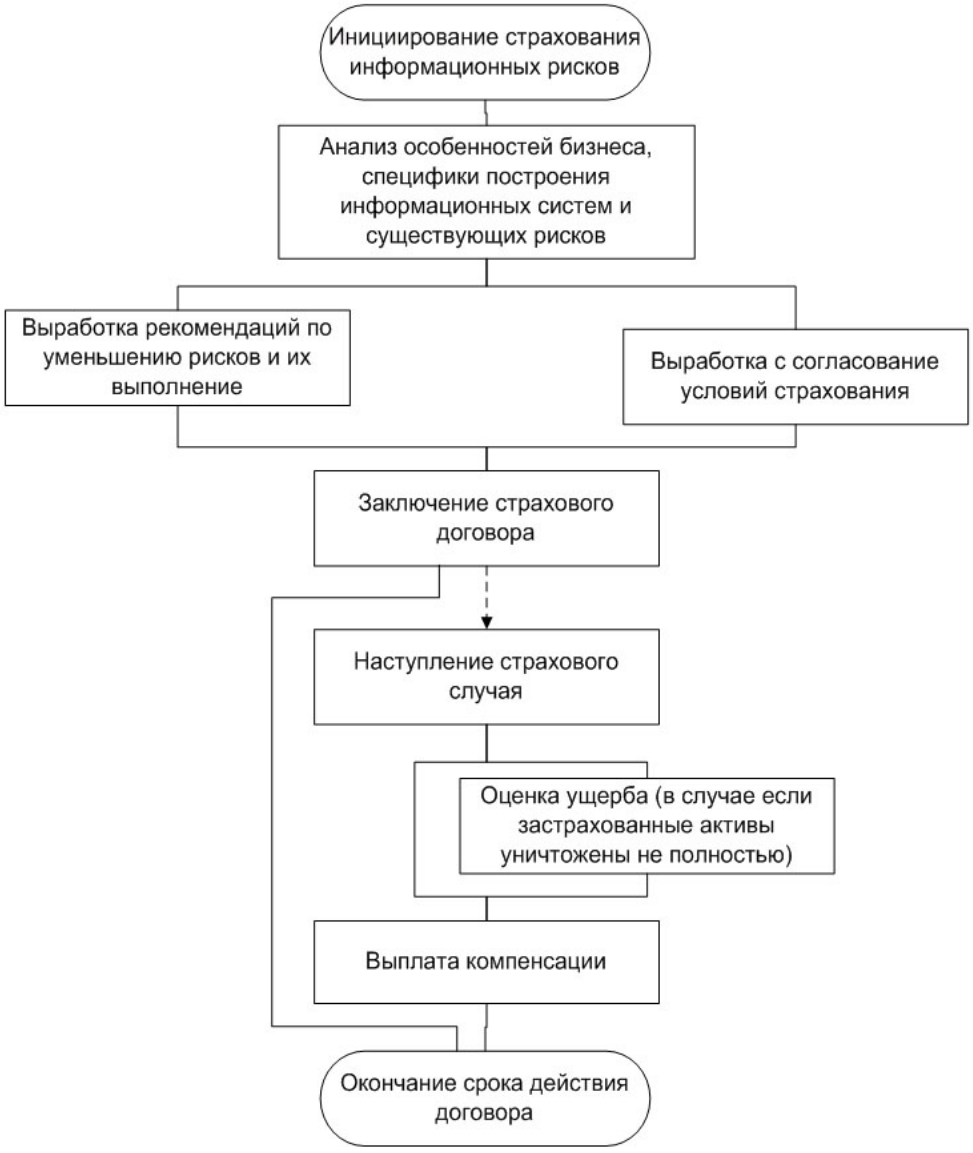
1. Предварительное обследование предприятия, анализ существующих рисков для информационной безопасности.

2. Формулирование рекомендаций по *уменьшению рисков* и реализация предприятием соответствующих мероприятий.

3. Согласование условий страхования и заключение договора.

4. Анализ ущерба и его расчет в денежном выражении в случае реализации застрахованных рисков.

5. Согласование и последующее осуществление страховых выплат, покрывающих ущерб.



Тема 4. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия

План:

1. Понятие комплексной системы безопасности предприятия.
2. Понятие аналитической работы, ее цели и задачи.
3. Стадии аналитической работы.
4. Методы аналитической работы
5.

1. ***Комплексная система безопасности предприятия***– совокупность взаимосвязанных организационных, правовых и технических мероприятий направленных на снижение и противодействие реальным и потенциальным , внутренним и внешним рискам и угрозам деятельности пред-

приятия, которые могут привести к существенным экономическим потерям, остановить или затормозить развитие предприятия.

К объектам обеспечения безопасности организации относится персонал, интеллектуальные, информационные, материальные, финансовые, технико-технологические и правовые ресурсы, а также стратегические, тактические и оперативные планы, систему управления, организационно-структурное построение, деловые внешние связи и заданные параметры функционирования организации.

Субъекты обеспечения безопасности организации подразделяются на внешние и внутренние. К внешним субъектам обеспечения безопасности организации относятся органы государственной власти и самоуправления, негосударственная система безопасности (в лице ее субъектов), эксперты, советники по безопасности и иные категории граждан, представители различных профессиональных и социальных групп, привлекаемые для обеспечения безопасности организации, СМИ, и различные общественные организации. К внутренним субъектам обеспечения безопасности относятся учредители, руководители всех уровней и персонал организации, служба (департамент, управление, отдел) безопасности, как субъект, непосредственно обеспечивающий и отвечающий за безопасность. Высшим коллегиальным органом, отвечающим за безопасность организации, является Совет по безопасности организации.

Построение и деятельность системы комплексного обеспечения безопасности организации осуществляется на основе ряда принципов, определяющих основополагающие требования к построению системы защиты. К ним относятся:

Принцип законности.
Принцип экономической целесообразности.
Принцип комплексности.
Принцип своевременности.
Принцип непрерывности.
Принцип активности.
Принцип обоснованности.
Принцип самостоятельности и ответственности.
Принцип совершенствования.
Принцип централизации управления.
Принцип взаимодействия и координации.
Принцип специализации и профессионализма.
Принцип конспирации и гласности.

2. В целях данных аналитических служб, призванных осуществлять информационное сопровождение управления в соответствующих сферах, наиболее четко просматривается информационно-вспомогательная природа информационной аналитики, упорядочивающая информационное пространство, оптимизирующая и направляющая движение информационных потоков, обеспечивающих сохранение накопленных информационных ресурсов и т.п.

Информационная аналитика выполняет прежде всего задачу качественно- содержательного преобразования информации, функционально пересекаясь в этом плане с научной (производство нового знания) и управленческой (разработка вариантов решений, сценариев) деятельностью.

Существенную роль играет и фактор времени. Информационная аналитика работает в режиме реального времени - времени жизнедеятельности своей предметной области (политики, экономики, бизнеса) и в соответствие с темпом необходимых управленческих реакций на динамику событий, происходящих в данной области.

Все больше аналитических задач решаются в режиме прямого информационного моделирования и наблюдения за управляемой сферой, минуя стадию анализа традиционных публикаций, информационный лаг которых (в данном случае интервал между событием, его отражением в публикациях и его включением в объекты для анализа) слишком велик.

Цель исследования — общая направленность исследования, ожидаемый конечный результат. Цель исследования указывает на характер задач исследования и достигается посредством их решения.

Задачи исследования — совокупность целевых установок, в которых формулируются основные требования к анализу и решению исследуемой проблемы.

Объект исследования — область практической деятельности, на которую направлен процесс исследования. Выбор объекта исследования определяет границы применения полученных результатов.

Предмет исследования — существенные свойства объекта исследования, познание которых необходимо для решения проблемы, в пределах которых объект изучается в данном конкретном исследовании.

Тематическое исследование — организационная форма аналитического слежения за состоянием и развитием обстановки, в рамках которой изучаются ее элементы с целью выработки тактических задач для практической деятельности.

Исследования в повседневной деятельности проводятся по мере накопления проблем. Исследуются: актуальность, важность, объективность, перспективность. Предметом исследования становятся события и процессы, развитие которых может повлиять на выбор форм и методов деятельности на определенном участке и в определенное время.

Средства аналитической работы — это законы и методы мыслительной деятельности, а также иные технические средства, на основе и с помощью которых осуществляется обработка фактических данных с более высоким качеством, позволяющим извлечь из нее все, что она может дать.

Формы аналитической работы — организационные особенности осуществления аналитической работы, обусловленные целями, средствами и результатами ее проведения, образующие систему аналитического слежения за состоянием и развитием обстановки.

Процесс аналитической работы — совокупность мыслительных операций, осуществляемых в определенной последовательности с использованием аналитических средств, приводящих к достижению целей и задач исследования.

Технология аналитической работы — получение нового знания (выводной информации), обеспечивающего сложный процесс исследования, имеющий определенную логическую последовательность.

Под ***проведением исследования*** понимается система взаимосвязанных рабочих операций, которые образуют технологический цикл отбора, группировки фактов о событиях, явлениях, процессах, где каждый факт обретает свое место и связан с предшествующими и последующими обстоятельствами в пространственно-временной и причинно-следственной зависимости.

Обобщение фактов, их научная обоснованная систематизация позволяют дать правильную оценку как всей совокупности фактов, так и каждому из них в отдельности.

Задание — правовой документ, определяющий состав, права и обязанности авторского коллектива в вопросах получения информации на тему исследования, консультаций со специалистами, реализации результатов, а также цели и задачи, объект и предмет, информационную базу, сроки и формы подготовки выходных документов.

План — организационный документ, устанавливающий последовательность осуществления этапов исследования, конкретизированных по исполнителям, срокам, формам подготовки выходных документов.

Методика исследования — организационный документ, в котором описывается система логических и методических правил проведения как в целом исследования, так и в рамках отдельных его направлений.

Постановка проблемы и ее предварительная проработка — начальный этап процесса аналитической работы, на котором окончательно определяются цели, задачи, предмет, объекты и информационная база исследования, прогнозируются главные результаты, способы и формы реализации.

Проблема исследования — разновидность вопроса, ответ на который не содержится в накопленном знании, и его поиск требует аналитических действий, отличных от информационного поиска.

Условия постановки проблем:

- когда результаты оперативной деятельности не соответствуют желаемым целям;
- когда ранее проверенные способы решения задач не могут быть использованы или не дают должного эффекта в новых условиях;
- когда обнаруживаются факты, не укладывающиеся в рамки существующих теоретических представлений;
- когда одна из частных теорий аналитической деятельности вступает в противоречие с более общей теорией данной деятельности.

Уяснение проблемы исследования — составная часть предварительной проработки проблемы, в рамках которой выявляются условия и предпосылки успешного проведения исследования: обоснованность постановки проблемы; актуальность и осуществимость ее разработки; возможность внедрения результатов в практику, а также определенность в целях, задачах, предмете, объекте и границах исследования.

Информационная база исследования — составная часть предварительной проработки проблемы, в рамках которой выявляется достаточность информационных материалов, пути и способы ее получения, составляется библиография по источникам.

Анализ собранных материалов в соответствии с целями и задачами исследования — это основной этап аналитической работы, на котором осуществляется осмысление материала, выработка новой выводной информации, формирование предложений по практическому их применению и документированию результатов исследования.

Анализ информации — совокупность методов формирования фактических данных, обеспечивающих их сравнимость (сопоставляемость), объективную оценку и выработку новой выводной информации.

Выработка новой информации — это извлечение содержания из всей массы исходных данных, отыскание причинно-следственных и пространственно-временных связей и взаимосвязей между сопоставляемыми сведениями.

Документирование результатов исследования — фиксация в установленном порядке результатов исследования с помощью системы обозначений, придающей описанию строгую форму, наглядность, логичность, краткость, ясность и отвечающей целям и задачам исследования.

Апробирование результатов исследования — проверочная процедура, направленная для выяснения качественных характеристик результатов исследования, возможностей реализации и внедрения их в практику.

Утверждение результатов исследования — согласовательная процедура, с помощью которой аналитический документ приобретает качества пригодности и обязательности для использования во всех заинтересованных сферах.

Реализация результатов исследования — это передача результатов исследования в удобной для внедрения форме в практику работы заинтересованных лиц, обеспечивающих повышение эффективности их деятельности.

Проверка, утверждение и внедрение результатов аналитической работы — это завершающий этап процесса исследования, на котором выявляются недостатки в аналитической работе, осуществляется их устранение и дается оценка качеству полученных результатов.

3. Процедура аналитической работы состоит из следующих этапов:

Этап 1. Общее знакомство с проблемой. Ознакомление с проблемой в целом, а также со смежными вопросами, изучение которых может оказаться полезным; составление общего плана работы с указанием срока выполнения, исполнителей и основных источников, которые предположительно могут быть использованы.

Этап 2. Определение используемых терминов и понятий.

Этап 3. Сбор фактов.

Этап 4. Истолкование фактов. Так кратко можно назвать процесс изучения и обработки фактов с целью выжать из них все, что они значат. Этот этап включает оценку, классификацию, анализ и уяснение фактов.

Этап 5. Построение гипотезы. Рабочие гипотезы, выдвигаемые на этом этапе, обычно связаны с какими-либо конкретными вопросами, отвечая на которые можно проверить сами гипотезы.. По мере изучения данного этапа мы открываем все новые полезные стороны рабочей гипотезы.

Гипотезу можно рассматривать как положение. Обычно отмечают три полезные стороны гипотезы:

— во-первых, тем самым облегчается уяснение проблемы. Установленное положение — прекрасное подспорье для памяти. Мы можем располагать значительными знаниями, помня определенное научное положение и не перегружая себя отдельными фактами;

— во-вторых, научное положение является основой для уяснения отдельных фактов или явлений, так как вскрывает существующую между ними связь. Мы можем осмыслить суть новых явлений, если выразим ее в знакомых нам понятиях;

— в-третьих, приемлемое научное положение всегда содержит некоторые моменты, выходящие за его рамки и образующие разумное и плодотворное основание для предвидения новых фактов и явлений.

Гипотеза — термин, прочно утвердившийся в научной литературе. Разведчики для обозначения рассматриваемого этапа чаще применяют термин “интеграция”, хотя эти два термина имеют не совсем одинаковое значение.

Этап 6. Выводы. На этом этапе производятся исследования, необходимые для доказательства или опровержения рабочих гипотез, выдвинутых на этапе 5, и формулируются окончательные выводы, являющиеся душой почти любого информационного документа. (“Выводы” — последний из девяти принципов информационной работы.)

Этап 7. Изложение. Составление документа, завершающее работу. Составитель информационного документа должен не только ясно представлять себе то, о чем он пишет, но и уметь выразить свои мысли в ясной форме.

4. ***Основным назначением*** всех аналитических методов является обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации. Существует широкий спектр специальных методов анализа: графические, табличные, матричные и т. п., например, диаграммы связи и матрицы участников, схемы потоков данных, временные графики, графики анализа визуальных наблюдений VIA (visual investigative analysis) и графики оценки результатов PERT (program evaluation review technique). Тем не менее следует отметить, что у каждого аналитика есть свой собственный метод анализа, который может быть как комбинацией вышеперечисленных методов, так и сугубо индивидуальным, уникальным методом аналитической работы.

С помощью диаграмм связей выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов. На диаграмме связей отмечают как наиболее прочные, так и вспомогательные связи между субъектами. Анализируются все связи без исключения, так как в ходе развития событий и получения дополнительной информации вспомогательные связи могут выступить на первый план. Для большей наглядности следует также указывать на диаграмме связи должностей (для физических лиц) или род деятельности (для юридических лиц).

Матрицы связей отражают частоту взаимодействия субъектов за определенный период времени. Такой метод анализа дополняет диаграммы связей, позволяет оценить характер взаимодействий между субъектами через частоту таких взаимодействий. При использовании этого метода анализа до его начала необходимо отделить маловажные и не имеющие отношения к делу, пусть даже частые, взаимодействия субъектов.

Схемы потоков информации позволяют оценить то, каким образом происходят события. С их помощью можно анализировать пути движения информации среди субъектов анализа, т. е. оце-

нивать положение каждого субъекта в общей группе и выявлять неустановленные связи между субъектами, используя определенную, специально подготовленную информацию как индикатор. Метод применим для отображения, например, физических процессов, взаимодействия юридических и физических лиц.

Временные графики используются для регистрации событий. Такая форма представления данных помогает не только эффективнее анализировать события, но и более рационально планировать меры противодействия.

Графики анализа визуальных наблюдений VIA являются составной частью графиков оценки результатов PERT. Оба графика составляются по принципу разбивки сложной операции на составные элементы. Такой принцип позволяет наглядно отражать ход событий. В зарубежных странах графики VIA и PERT применяются для анализа тяжких преступлений и террористической деятельности, для повышения эффективности работы предприятий, а также аналитиками служб безопасности для нужд ИАС фирм. В обоих графиках принята одна и та же система символов: события представлены треугольниками и кругами, причем треугольники отмечают начало и конец события, а также наиболее важные моменты операции. Отличием этих типов графиков является то, что график VIA представляет собой схему визуальных наблюдений в процессе одиночного события, а график PERT отражает общий ход событий, является более общим методом анализа. Графики VIA и PERT могут иметь различную степень детализации событий. С их помощью легко вычленить определенную схему в действиях субъектов, что значительно облегчит процесс построения версий. Графики PERT широко применяются при таком широко распространенном методе анализа, как изучение реальных дел с целью поиска аналогий. Такой метод позволяет определить возможные сценарии, по которым события реально развивались в предшествующий период. Основная идея этого метода состоит в том, что все события рано или поздно повторяются в силу схожести целей, средств и обстоятельств. Разбор и анализ ситуаций, имевших место в прошлом, позволяет на раннем этапе выявить подлинный характер происходящего за счет совпадения с типичными схемами.

В настоящее время в работе ИАС широко используются возможности современной вычислительной техники. Это относится не только к созданию баз данных по тематике аналитической работы, но и непосредственно к процессу анализа. Статистический анализ в подавляющем большинстве случаев не выполняется вручную, для этого должны применяться специальные пакеты программ статистической обработки данных, предназначенные для аналитической работы. Такие программы используются зарубежными специалистами при анализе уже достаточно длительное время и с большим успехом.

В последнее время для аналитической работы все чаще применяются так называемые экспертные системы (expert systems), которые, являясь практическим приложением искусственного интеллекта, оказывают огромную помощь при анализе, а в ряде случаев могут даже заменить собой аналитика. Они представляют собой класс компьютерных программ, которые выдают советы, проводят анализ, выполняют классификацию, дают консультации и ставят диагноз. Экспертные системы не только выполняют все эти функции, но и на каждом шаге могут объяснить аналитику причину той или иной рекомендации и последовательность анализа. Широкое использование таких систем в зарубежных странах объясняется тем фактом, что аналитические задачи, как и все задачи, требующие дедуктивных рассуждений, решаются компьютером не хуже, чем человеком, а в ряде случаев – быстрее и надежнее. В отличие от человека-аналитика у экспертных систем нет предубеждений, они не делают поспешных выводов, не поддаются влиянию внешних факторов. Такие системы работают систематизировано, рассматривая все детали, выбирая наилучшую альтернативу из всех возможных. Несомненным преимуществом экспертных систем является и то, что, будучи введены в машину один раз, знания сохраняются навсегда, как бы обширны они ни были.

Теоретически экспертные системы по мере своего развития и расширения проходят три стадии:

1) ассистент – система освобождает человека-аналитика от рутинной и однообразной аналитической работы, позволяя заниматься только самыми важными и ответственными вопросами;

2) коллега – система участвует в решении проблемы на равных с человеком, общение с системой представляет собой постоянный диалог;

3) эксперт – уровень знаний системы во много раз превосходит уровень знаний человека, так как знания системы представляют собой постоянно пополняемую совокупность знаний многих ведущих экспертов в этой области.

Реально в настоящее время применяются экспертные системы первого уровня – облегчающие работу аналитика. Такие системы накапливают знания и опыт наиболее квалифицированных экспертов-аналитиков. С помощью этих знаний пользователь с обычной квалификацией может решать различные аналитические задачи столь же успешно, как и сами эксперты. Это происходит за счет того, что система в своей работе воспроизводит ту же схему рассуждений, что и человек-эксперт при анализе проблемы.

Второй уровень экспертных систем пока не достигнут в силу больших практических трудностей.

Третий уровень экспертных систем пока существует лишь в проекте.

Экспертные системы позволяют копировать и распространять знания, делая уникальный опыт нескольких экспертов-аналитиков доступным широким кругам рядовых специалистов. То есть такие системы имитируют деятельность человека-эксперта. Однако эти системы имеют существенные недостатки – большинство экспертных систем не вполне пригодны для применения конечным пользователем, они рассчитаны в первую очередь на использование теми экспертами, которые создавали их базы знаний. Пользователь экспертной системы не только должен иметь определенные навыки работы с такими системами, но и представлять себе логику ее построения. К недостаткам можно отнести и то, что приведение знаний, полученных от эксперта, к виду, обеспечивающему их эффективную машинную реализацию, все еще остается достаточно сложной задачей. Экспертные системы еще не способны самообучаться, не обладают интуицией и здравым смыслом, которые использует человек-аналитик при отсутствии формальных методов решения или аналогов таких задач.

Тема 5. Методологические основы системы безопасности предприятия

План:

1 Коммерческая тайна: разработка и цели и задачи

2. Существующие методики сбора, анализа и обобщения сведений.

3. Конфиденциальность сведений.

1. ***Коммерческая информация*** содержит сведения о финансово- экономическом положении предприятия (бухгалтерская отчетность), кредитах и банковских операциях, о заключаемых договорах и контрагентах, структуре капиталов и планах инвестиций, стратегических планах маркетинга, анализе конкурентоспособности собственной продукции, клиентах, планах производственного развития, деловой переписке и проч. Информация представляет определенную ценность для предпринимателя, разглашение тех или иных сведений может создать угрозы экономической безопасности предприятия. Поэтому информацию необходимо разделить на три группы: информация для открытого пользования любым потребителем в любой– форме; информация ограниченного доступа — только для органов, имеющих– соответствующие законодательно установленные права (милиция, налоговая полиция, прокуратура); информация только для работников (либо руководителей) фирмы.– Информация, относящаяся ко второй и третьей группам, является конфиденциальной и имеет ограничения в распространении. Конфиденциальная информация — это документированная информация, т.е. зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать, доступ к которой ограничивается в соответствии с законодательством РФ. Законом охраняется государственная, служебная, банковская, военная, коммерческая тайна. Часть коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Коммерческая тайна – это *конфиденциальность* информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных

расходов, сохранить положение на рынке товаров, *работ*, услуг или получить иную коммерческую выгоду. Именно таким образом определяет понятие "*коммерческая тайна*" Федеральный закон "О коммерческой тайне" от 29 июля 2004 г. № 98-ФЗ. *Информация*, составляющая *коммерческую тайну*, – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен *режим коммерческой тайны*.

Меры *по* охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- определение перечня информации, составляющей *коммерческую тайну*;
- ограничение доступа к информации, составляющей *коммерческую тайну*, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, которые получили доступ к информации, составляющей *коммерческую тайну*, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей *коммерческую тайну*, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- нанесение на материальные носители (документы), содержащие информацию, составляющую *коммерческую тайну*, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

После соблюдения указанных мер, *режим коммерческой тайны* считается установленным. Меры *по* охране конфиденциальности информации признаются разумно достаточными, если:

1. исключается доступ к информации, составляющей *коммерческую тайну*, любых лиц без согласия ее обладателя;
2. обеспечивается возможность использования информации, составляющей *коммерческую тайну*, работниками и передачи ее контрагентам без нарушения режима *коммерческой тайны*. Под контрагентом понимается сторона гражданско-правового договора, которой обладатель информации, составляющей *коммерческую тайну*, передал эту информацию.

Специфика режима *коммерческой тайны* предполагает и соответствующую ответственность за нарушение этого режима. В зависимости от характера нарушения и нарушителя ответственность может быть различная.

Во-первых, ***дисциплинарная***. Согласно Трудовому кодексу, трудовой договор может быть расторгнут *по* инициативе работодателя в связи с разглашением охраняемой законом *коммерческой тайны*, ставшей известной работнику в связи с исполнением им трудовых обязанностей.

Во-вторых, ***гражданско-правовая***. Лица, незаконными методами получившие информацию, которая составляет *коммерческую тайну*, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших *коммерческую тайну* вопреки трудовому или гражданско-правовому договору. Под убытками понимаются *расходы*, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного *права* (реальный *ущерб*), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода).

В-третьих, ***административная***. Ст. 13.14 КоАП устанавливает, что разглашение информации, *доступ* к которой ограничен федеральным законом (за исключением случаев, когда разглашение такой информации влечет уголовную ответственность), лицом, получившим *доступ* к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключе-

нием деяний, признаваемых КоАП недобросовестной конкуренцией, влечет наложение административного штрафа на граждан в размере от 500 до 1 000 рублей; на должностных лиц – от 4 000 до 5 000 рублей.

В-четвертых, ***уголовная***. Ст. 183 УК РФ предусматривает, что собирание сведений, составляющих *коммерческую тайну*, путем похищения документов, подкупа или угроз, а равно иным незаконным способом, наказывается штрафом в размере до 80 000 рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. *Аудит* состояния информационной безопасности на предприятии представляет собой экспертное обследование основных аспектов информационной безопасности, их проверку на соответствие определенным требованиям. В некоторых случаях под аудитом информационной безопасности подразумевается проверка защищенности отдельных элементов информационной инфраструктуры предприятия (сегментов его сети, отдельных серверов, баз данных, Интернет-сайтов и т.п.) и надежности средств защиты информации (межсетевых экранов, систем обнаружения вторжений и т.п.). Однако мы в дальнейшем исходим из того, что *аудит* информационной безопасности является комплексным (по возможности, исчерпывающим) исследованием всех аспектов информационной безопасности (как технических, так и организационных) в контексте всей хозяйственной деятельности предприятия с учетом действующей политики информационной безопасности, объективных потребностей предприятия и требований, предъявляемых третьими лицами (государством, контрагентами и т.п.).

Различают два основных вида аудита: внутренний (проводимый исключительно силами сотрудников предприятия) и внешний (осуществляемый сторонними организациями).

Целями аудита могут быть:

- установление степени защищенности информационных ресурсов предприятия, выявление недостатков и определение направлений дальнейшего развития системы защиты информации;
- проверка руководством предприятия и другими заинтересованными лицами достижения поставленных целей в сфере информационной безопасности, выполнения требований политики безопасности;
- контроль эффективности вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности;
- сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам).

Одной из стратегических задач, решаемых при проведении аудита информационной безопасности и получении соответствующего сертификата, является демонстрация надежности предприятия, его способности выступать в качестве устойчивого партнера, способного обеспечить комплексную защиту информационных ресурсов, что может быть особенно важно при осуществлении сделок, предполагающих обмен конфиденциальной информацией, имеющей большую *стоимость* (финансовыми сведениями, конструкторско-технологической документацией, результатами *НИОКР* и т.п.).

В том случае, если *аудит* является внутренним, группу аудиторов необходимо сформировать из числа таких специалистов, которые сами не являются разработчиками и администраторами используемых информационных систем и средств защиты информации и не имели отношения к их внедрению на данном предприятии.

Как правило, предприятие может прибегать к помощи внешних аудиторов с целью:

- повышения объективности, независимости и профессионального уровня проверки;
- получения заключений о состоянии информационной безопасности и соответствии международным стандартам от независимых аудиторов.

Компании, специализирующиеся на проведении аудитов, могут осуществлять проверки состояния информационной безопасности на соответствие таким общепризнанным стандартам и требованиям, как:

• *ISO 15408*: *Common Criteria* for Information Technology *Security Evaluation* (Общие критерии *оценки безопасности* информационных технологий);

• *ISO 17799* (BS 7799): Code of Practice for Information *Security Management* (Практические правила *управления информационной безопасностью*);

• BSI\IT: Baseline Protection Manual (Руководство базового уровня по защите информационных технологий Агентства информационной безопасности Германии);

• COBIT: Control Objectives for Information and related Technology (Основные цели для информационных и связанных с ними технологий);

• Требованиям Руководящих документов ФСТЭК РФ, ФСБ или других государственных органов

• и других документов (таких как SAC, COSO, *SAS* 55/78).

При этом организация, осуществляющая внешний *аудит*, должна отвечать определенным требованиям:

• иметь право (лицензию) на выдачу заключений о соответствии определенным требованиям (например, аккредитацию UKAS – United Kingdom Accreditation Service);

• сотрудники должны иметь право доступа к информации, составляющей государственную и военную тайну (если такая информация имеется на проверяемом предприятии);

• обладать необходимыми программными и аппаратными средствами для исчерпывающей проверки имеющегося у предприятия программного и аппаратного обеспечения.

Основными этапами проведения аудита являются:

• инициирование проведения аудита;

• непосредственно осуществление сбора информации и проведение обследования аудиторами;

• анализ собранных данных и выработка рекомендаций;

• подготовка аудиторского отчета и аттестационного заключения.

Аудит должен быть инициирован руководством предприятия с достаточно четко сформулированной целью на определенном этапе развития информационной системы или системы обеспечения информационной безопасности предприятия (например, после завершения одного из этапов внедрения). В случае если *аудит* не является комплексным, на начальном этапе необходимо определить его непосредственные границы:

• перечень обследуемых информационных ресурсов и информационных систем (подсистем);

• перечень зданий, помещений и территорий, в пределах которых будет проводиться аудит;

• основные угрозы, средства защиты от которых необходимо подвергнуть аудиту;

• элементы системы обеспечения информационной безопасности, которые необходимо включить в процесс проверки (организационное, правовое, программно-техническое, аппаратное обеспечение);

Основная стадия – **проведение аудиторского обследования и сбор информации** – как правило, должно включать в себя:

• анализ имеющейся политики информационной безопасности и другой организационной документации;

• проведение совещаний, опросов, доверительных бесед и интервью с сотрудниками предприятия;

• проверку состояния физической безопасности информационной инфраструктуры предприятия;

• техническое обследование информационных систем – программных и аппаратных средств (инструментальная проверка защищенности).

Прежде чем приступить собственно к аудиту информационной безопасности, аудиторам (в частности, если проводится внешний *аудит*) необходимо ознакомиться со структурой предприятия, его функциями, задачами и основными бизнес-процессами, а также с имеющимися информационными системами (их составом, функциональностью, процедурами использования и ролью на предприятии). На начальном этапе аудиторы принимают решения о том, насколько глубоко и детально будут исследованы отдельные элементы информационной системы и системы защиты

информации. Также необходимо заранее скоординировать с пользователями информационных систем процедуры проверки и тестирования, требующие ограничения доступа пользователей (такие процедуры по возможности должны проводиться в нерабочее время или в периоды наименьшей загрузки информационной системы).

Качественный **анализ действующей на предприятии политики безопасности** является отправной точкой для проведения аудита. Одна из первых задач комплексного аудита — установление того, в какой степени действующая политика соответствует объективным потребностям данного предприятия в безопасности, могут ли действия в рамках данной политики обеспечить необходимый уровень защищенности информации и средств ее обработки, хранения и передачи. Это, в свою *очередь*, может потребовать проведения дополнительной оценки значимости основных информационных активов предприятия, их уязвимости, а также существующих рисков и угроз. *Анализ* политики также может включать оценку таких ее характеристик, как:

- полнота и глубина охвата всех вопросов, а также соответствие содержания политик нижнего уровня целям и задачам, установленным в политиках верхнего уровня;
- понятность текста политики для людей, не являющихся техническими специалистами, а также четкость формулировок и невозможность их двойного толкования;
- актуальность всех положений и требований политики, своевременность учета всех изменений, происходящих в информационных системах и бизнес-процессах.

После проверки основных положений политики безопасности в процессе аудита могут быть изучены (проверены) действующие классификации информационных ресурсов по степени критичности и конфиденциальности, а также другие документы, имеющие *отношение* к обеспечению информационной безопасности:

- организационные документы подразделений предприятия (положения об отделах, должностные инструкции);
- инструкции (положения, методики), касающиеся отдельных бизнес-процессов предприятии;
- кадровая документация, обязательства о неразглашении сведений, данные сотрудниками, свидетельства о прохождении обучения, профессиональной сертификации, аттестации и ознакомлении с действующими правилами;
- техническая документация и пользовательские инструкции для различных используемых программных и аппаратных средств (как разработанных самим предприятием, так и приобретенных у сторонних поставщиков): межсетевых экранов, маршрутизаторов, операционных систем, антивирусных средств, систем управления предприятием и т.п.

Основная работа аудиторов в процессе сбора информации заключается в изучении фактически предпринимаемых мер по обеспечению защиты информационных активов предприятия, таких как:

- организация процесса обучения пользователей приемам и правилам безопасного использования информационных систем;
- организация работы администраторов информационных и телекоммуникационных систем и систем защиты информации (правильность использования программных и аппаратных средств администрирования, своевременность создания и удаления учетных записей пользователей, а также настройки их прав в информационных системах, своевременность замены паролей и обеспечение их соответствия требованиям безопасности, осуществление резервного копирования данных, ведение протоколов всех производимых в процессе администрирования операций, принятие мер при выявлении неисправностей и т.п.);
- организация процессов повышения квалификации администраторов информационных систем и систем защиты информации;
- обеспечение соответствия необходимых (в соответствии с политикой безопасности и должностными обязанностями) прав пользователей информационных систем и фактически имеющихся;
- организация назначения и использования специальных ("суперпользовательских") прав в информационных системах предприятия;

• организация работ и координации действий при выявлении нарушений информационной безопасности и восстановлении работы информационных систем после сбоев и нападений (практическое выполнение "аварийного плана");

• предпринимаемые меры антивирусной защиты (надлежащее использование антивирусных программ, учет всех случаев заражения, организация работы по устранению последствий заражений и т.п.);

• обеспечение безопасности приобретаемых программных и аппаратных средств (наличие сертификатов и гарантийных обязательств, поддержка со стороны поставщика при устранении выявленных недостатков и т.п.);

• обеспечение безопасности самостоятельно разрабатываемого программного обеспечения (наличие необходимых требований в проектной документации информационных систем, качество программной реализации механизмов защиты и т.п.);

• организация работ по установке и обновлению программного обеспечения, а также контроля за целостностью установленного ПО;

• предпринимаемые меры по обеспечению учета и сохранности носителей информации (дисков, дискет, магнитных лент и т.п.), а также по их безопасному уничтожению после окончания использования;

• эффективность организации взаимодействия сотрудников предприятия – пользователей информационных систем – со службой информационной безопасности (в частности, по вопросам реагирования на инциденты и устранения их последствий).

Тема 6. Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов

План:

1. Корпоративная информационная система
2. Основные задачи и функции службы безопасности предприятия
3. Состав службы безопасности

1. Информационные системы повышенной сложности, такие как корпоративные информационные системы (КИС), как правило, состоят из нескольких подсистем, решающих конкретные задачи. При построении КИС следует увязывать подсистемы в единый комплекс, придерживаясь ряда основополагающих принципов:

использования общепринятых стандартов, поддерживаемых основными фирмами – производителями программного обеспечения;

применения программного обеспечения достаточной производительности, чтобы его не приходилось менять при увеличении мощности и количества используемого оборудования. Это качество называется масштабируемостью программного обеспечения;

соблюдения принципа многозвенности, означающего, что каждый уровень системы (клиент, веб-сервер, сервер приложений, сервер баз данных) реализует функции, наиболее ему присущие;

реализации принципа аппаратно-платформенной независимости и системного программного обеспечения;

осуществления принципа коммуникативности, когда различные уровни системы могут взаимодействовать между собой как по данным, так и по приложениям.

Общепринятым подходом к решению вопросов защиты является использование в корпоративной сети, имеющей выход в публичную сеть Интернет, следующей стратегии управления доступом между двумя сетями:

весь трафик, как из внутренней сети во внешний мир, так и наоборот, должен контролироваться корпоративной системой;

через систему может пройти только авторизованный трафик, который определяется стратегией защиты.

Межсетевой экран – это механизм, используемый для защиты доверенной сети (внутренняя сеть организации) от сети, не имеющей доверия, например Интернета.

Одной из существенных особенностей КИС является реализация в ней принципа централизованного управления, благодаря чему возможно выполнение таких важных функций, как:

авторизация и управление распределенной информацией в масштабах всего предприятия;

возможность централизованной аутентификации и управление контролем доступа ко всем веб-серверам вне зависимости от их платформ (централизованное управление веб-пространством за счет связи веб-серверов в одно логическое веб-пространство);

управление доступом к персональной информации пользователей;

централизованное кросс-платформенное управление учетными записями пользователей;

управление цифровыми сертификатами для электронного бизнеса;

централизованное кросс-платформенное управление доступом пользователей к информационным ресурсам;

управление рисками на предприятии, позволяющее системным администраторам контролировать все несанкционированные вторжения на предприятие.

2. Основными ***задачами*** службы безопасности предприятия являются:

обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;

организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;

организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;

предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;

выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством;

обеспечение личной безопасности руководства и ведущих сотрудников и специалистов; • оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Общие функции службы безопасности:

организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;

руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов;

разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований инструкции по защите коммерческой тайны;

изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности компании и ее клиентов, партнеров, смежников;

организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;

разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;

организует и регулярно проводит учебу сотрудников компании и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход;

ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

3. Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

отдела режима и охраны, в составе сектора режима и сектора охраны;

специального отдела в составе сектора обработки секретных документов и сектора обработки документов с грифом «Коммерческая тайна»;

инженерно-технической группы;

группы безопасности внешней деятельности.

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:

требовать от всех сотрудников предприятия, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;

вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности обязаны:

осуществлять контроль за соблюдением «Инструкции по защите коммерческой тайны»;

докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;

не допускать неправомерного ознакомления с документами и материалами с грифом

В некоторых компаниях начали создаваться службы, отвечающие за обеспечение безопасности конфиденциальной информации. Безусловно, структура и состав таких служб зависит от финансового состояния компании. Ибо содержание подобных служб требует немалых финансовых затрат. Однако в настоящее время есть компании, которые в состоянии содержать такие структуры, обеспечивая тем самым безопасность конфиденциальной информации, а значит, и ее экономическое благополучие. И в дальнейшем количество таких компаний будет постоянно расти. Возглавлять данную службу должен начальник службы безопасности информации. Для мелких компаний — помощник начальника службы безопасности компании по информационной безопасности. Эта должность может быть штатной, или ее можно занимать по совместительству.

В службе безопасности должны быть должностные лица, отвечающие первоначально за отдельные направления защиты. Ими могут быть:

специалист по обеспечению безопасности информации в выделенных помещениях компании

специалист по обеспечению безопасности информации на объектах вычислительной техники компании;

специалист по обеспечению безопасности связи.

Кроме того, в каждом выделенном помещении должны быть назначены ответственные по обеспечению безопасности информации. Помимо этого, ответственные назначаются на ка-ждый

объект вычислительной техники. Что касается безопасности связи, то здесь должны быть ответственные за обеспечение безопасности каждого вида связи (телефонной, телеграфной, факсимильной, при передаче данных.

Тема 7. Защита информации при проведении совещаний и переговоров по конфиденциальным вопросам, приеме посетителей.

План:

1. Защита информации в помещениях
2. Защита от перехвата информации с телефонных линий

1. Под помещением понимается служебное помещение, в котором ведутся разговоры (переговоры) конфиденциального характера. К таким помещениям относятся комнаты где ведутся деловые переговоры, содержащие конфиденциальную информацию.

Основная цель обеспечения безопасности конфиденциальной информации в переговорных комнатах — исключить доступ к ее содержанию при проведении переговоров (разговоров). Первостепенными задачами обеспечения безопасности информации являются:

1. Защита информации от утечки по акустическому каналу (АК).
2. Защита информации от утечки по виброакустическому каналу (ВАК).
3. Защита информации от утечки за счет электроакустического преобразования (ЭАП).
4. Защита информации от утечки за счет высокочастотного навязывания (ВЧН).
5. Защита информации от утечки по оптическому каналу (ОК).

Несанкционированный доступ к конфиденциальной информации по акустическому каналу утечки может осуществляться:

путем непосредственного прослушивания;

при помощи технических средств.

Непосредственное прослушивание переговоров (разговоров) злоумышленником может быть осуществлено:

через дверь;

через открытое окно

через стены, перегородки;

через вентиляционные каналы.

Несанкционированный доступ к содержанию переговоров (разговоров) злоумышленник может осуществить и при помощи технических средств, таких как:

направленные микрофоны;

проводные микрофоны;

радиомикрофоны;

устройство «Электронное ухо».

Рекомендации по защите информации:

1. Важен выбор места для оборудования переговорной комнаты. Ее целесообразно разместить по возможности на верхних этажах. Желательно, чтобы комната для переговоров не имела окон или же они выходили во двор.

2. В комнате для переговоров не должно быть телевизоров, приемников, ксероксов, настенных электрических часов, телефонных аппаратов.

3. Вход в переговорную комнату должен быть оборудован тамбуром, а внутренняя сторона тамбура обита звукоизоляционным материалом. Необходимо помнить, что незначительная щель (единицы миллиметров) многократно снижает звукоизоляцию.

4. При наличии в комнате для переговоров вентиляционных каналов нужно позаботиться, чтобы они были оборудованы специальными решетками, позволяющими закрывать отверстие вентиляционного канала при ведении переговоров и открывать его, когда переговоры не ведутся.

5. Если в комнате имеются окна, то должны быть приняты следующие меры предосторожности:

проводить переговоры разрешается при закрытых форточках;

на окнах должны быть шторы или жалюзи

оконные стекла должны быть оборудованы вибродатчиками.

6. При наличии в переговорной комнате телефонного аппарата должны быть приняты меры защиты. В телефонных аппаратах с дисковым номеронабирателем целесообразно использовать фильтр «Корунд-М», обеспечивающий затухание сигнала утечки порядка 80 дБ. Для защиты от высокочастотного навязывания рекомендуется подключить параллельно микрофону (для любых телефонных аппаратов) конденсатор емкостью С = 0,01 — 0,05 мкФ. На практике могут встречаться и более сложные схемы защиты звонковой и микрофонной цепи телефонных аппаратов.

7. Для защиты от проводных микрофонов, использующих для передачи информации сеть электропитания в 220 В, рекомендуется использовать генератор типа «Соната-С1», который имеет хорошие тактико-технические характеристики и эффективно выполняет функции защиты.

8. Для защиты переговорных комнат от специальных технических средств необходимо воспользоваться генератором виброакустического шума «Соната-АВ» и генератором радиопомех «Баррикада-1».

2. Защита телефонных переговоров является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности любой организации (фирмы)

Для прослушивания телефонных переговоров наиболее часто используются электронные устройства перехвата речевой информации (телефонные закладки), несанкционированно подключаемые к телефонным линиям последовательно (в разрыв одного из проводов), параллельно (одновременно к двум проводам).

Методы защиты информации на энергетическом уровне

При защите телефонных разговоров на энергетическом уровне осуществляется подавление электронных устройств перехвата информации с использованием активных методов и средств. К основным относятся следующие методы:

«синфазной» низкочастотной маскирующей помехи;

высокочастотной маскирующей помехи;

«ультразвуковой» маскирующей помехи;

низкочастотной маскирующей помехи;

повышения напряжения;

понижения напряжения;

компенсационный;

«выжигания».

Метод «синфазной» маскирующей низкочастотной помехи

Суть метода заключается в подаче во время разговора в каждый провод телефонной линии согласованных по амплитуде и фазе относительно нулевого провода электросети 220 В маскирующих сигналов речевого диапазона частот (маскирующего низкочастотного шума). Вследствие согласования по амплитуде и фазе в телефонном аппарате, подключаемом параллельно телефонной линии, эти сигналы компенсируют друг друга и не приводят к искажению полезного сигнала, т.е. не ухудшают качество связи. В любых устройствах, подключаемых к одному телефонному проводу (как последовательно, так и через индукционный датчик), сигнал помехи не компенсируется и «накладывается» на полезный сигнал. А так как его уровень значительно превосходит полезный сигнал, то перехват передаваемой информации становится невозможным.

Метод высокочастотной маскирующей помехи

Метод высокочастотной маскирующей помехи заключается в подаче во время разговора в телефонную линию маскирующего сигнала помехи в диапазоне высоких частот звукового диапазона (маскирующего высокочастотного шума). Частоты маскирующих сигналов помехи подбираются таким образом, чтобы после прохождения низкочастотного усилителя или селективных цепей модулятора телефонной закладки их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии), но в то же время, чтобы они не ухудшали качество связи.

Метод «ультразвуковой» маскирующей помехи

Метод «ультразвуковой» маскирующей помехи аналогичен рассмотренному выше. От-личие состоит в том, что частота сигнала помехи находится в диапазоне от 20-30 кГц до 50-100 кГц, что намного упрощает схему устройства подавления, но при этом эффективность данного метода по сравнению с методом высокочастотной маскирующей помехи ухудшается.

Метод низкочастотной маскирующей помехи При использовании метода в линию при положенной телефонной трубке подается маскирующий низкочастотный сигнал помехи. Этот метод применяется для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки (заполнению-памяти) в режиме записи шума, то есть при отсутствии полезного сигнала.

Метод повышения напряжения

Во время разговора и используется для ухудшения качества функционирования телефонных закладок за счет перевода их передатчиков в нелинейный режим работы.

Метод понижения напряжения предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Компенсационный метод Компенсационный метод используется для маскировки (скрытия) речевых сообщений, передаваемых абонентом по телефонной линии. Данный метод обладает высокой эффективностью подавления всех известных средств несанкционированного съема информации, подключаемых к линии на всем участке телефонной линии от одного абонента до другого. Суть метода заключается в следующем: перед началом передачи скрываемого сообщения по специальной команде абонента на приемной стороне включается генератор шума, подающий в телефонную линию, маскирующую шумовую помеху (как правило, «цифровой» шумовой сигнал) речевого диапазона частот, которая в линии «смешивается» с передаваемым сообщением.

Тема 8. Технологические системы защиты и обработки конфиденциальных документов

План:

1. Назначение технологической системы обработки и хранения конфиденциальных документов
2. Виды технологических систем защиты и обработки конфиденциальной информации
3. Служба конфиденциальной информации

1. Под технологической системой обработки и хранения конфиденциальных документов понимается упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих перед функциональными элементами (стадиями) документопотока. Технология обработки и хранения конфиденциальных и открытых документов базируется на единой научной и методической основе, призванной решать задачи обеспечения документированной информацией управленческие и производственные процессы. Одновременно технологическая система обработки и хранения конфиденциальных документов решает и другую не менее важную задачу — обеспечение защиты носителей информации и самой информации от потенциальных и реальных угроз их безопасности.

В отличие от открытых документов к обработке конфиденциальных документов предъявляются следующие серьезные требования:

• централизация всех стадий, этапов, процедур и операцийпо обработке и хранению конфиденциальных документов;

• учет всех без исключения конфиденциальных документов;

• операционный учет технологических действий, производимых с традиционным (бумажным) или электронным носителем (в том числе чистым) и документом, учет каждого факта «жизненного цикла» документа;

• обязательный контроль вторым работником службы КД правильности выполнения учетных операций;

• учет и обеспечение сохранности не только документов,но и учетных форм;

• ознакомление или работа с документом только на основании письменной санкции (разрешения) полномочного руководителя, письменного фиксирования всех обращений персонала к документу;

• обязательная подпись руководителей, исполнителей и технического персонала при выполнении любых действий с документом в целях обеспечения персональной ответственности сотрудников фирмы за сохранность носителя и конфиденциальность информации;

• строгий контроль выполнения персоналом введенных в фирме правил работы с конфиденциальными документами, делами и базами данных, обязательными для всех категорий персонала;

• систематические (периодические и разовые) проверки наличия документов у исполнителей, в делах, базах данных, на машинных носителях и т.д., ежедневный контроль сохранности, комплектности, целостности и местонахождения каждого конфиденциального документа;

• коллегиальность процедуры уничтожениядокументов, дели баз данных;

• письменное санкционирование полномочным руководителем процедур копирования и размножения бумажных и электронных конфиденциальных документов, контроль технологии выполнения этих процедур.

Технологическая система обработки и хранения конфиденциальных документов распространяется не только на управленческую (деловую) документацию, но и на конструкторские, технологические, научно-технические и другие аналогичные документы, публикации, нормативные материалы и др., хранящиеся в специальных библиотеках, информационных центрах, ведомственных архивах, документированную информацию, записанную на любом типе носителя информации.

2. Технологические системы обработки и хранения конфиденциальных документов могут быть традиционными, автоматизированными и смешанными.

Традиционная (делопроизводственная) система основывается на ручных методах работы человека с документами и является универсальной. Она надежно, долговременно обеспечивает защиту документированной информации как в обычных, так и в экстремальных ситуациях. В связи с этим стадии защищенного документооборота в большинстве случаев технологически реализуются методами и средствами именно традиционной системы обработки и хранения конфиденциальных документов, а не автоматизированной. Система одинаково эффективно оперируеткактрадиционными (бумажными) документами, так и документами машиночитаемыми, факсимильными и электронными. Трудоемкость множества технических и формально-логических процедур и операций обычно снижается за счет включения в технологический процесс организационной и вычислительной техники, что в целом не меняет тип системы. Вместе с тем система характеризуется низкой степенью оперативности доставки документов потребителям информации, невысокой эффективностью справочной, поисковой и контрольной работы по документам, потребностью в значительном количестве персонала, обслуживающего систему.

Традиционная технологическая система обработки и хранения конфиденциальных документов лежит в основе широко известного понятия «делопроизводство» или «документационное обеспечение управления» (в его узком, но часто встречающемся в научной литературе понимании как синонима делопроизводства). С другой стороны, делопроизводство часто рассматривается в качестве организационно-правового и технологического инструмента построения документационного обеспечения управления, с чем, на наш взгляд, трудно не согласиться.

Автоматизированная технологическая система обработки и хранения конфиденциальных документов по сравнению с аналогичными системами, оперирующими общедоступной информацией, имеет ряд принципиальных особенностей:

• архитектурно компьютеры, обрабатывающие значительные объемы конфиденциальной информации, могут объединяться в локальную сеть как в рамках службы КД, так и с охватом руководителей и основных специалистов; однако в любом варианте локальная сеть базируется на главном компьютере (сервере), находящемся у системного администратора службы КД; автоматизированные рабочие места, рабочие станции могут быть увязаны в локальную сеть только по вертикали;

• в некрупных фирмах конфиденциальная информация обрабатывается на уровне первого руководителя и его референта на единичном защищенном компьютере, не имеющем выхода в какую-либо локальную сеть;

• обязательное наличие иерархической и утвержденной первым руководителем фирмы системы разграничения доступа к информации, хранящейся как в машинных массивах, так и на магнитных носителях вне ЭВМ; охват системой разграничения доступа не только персонала фирмы, но и персонала службы КД;

• закрепление за каждым пользователем строго определенного состава массивов электронной информации и магнитных носителей; исключение возможности для пользователя «покопаться» в базе данных системы;

• автоматизированное выполнение пользователями операций справочного и поискового обслуживания, составления и иногда изготовления документов, контроля исполнения документов, работы с электронными документами, факсами и электронными налогами бумажных документов;

• сохранение информационной базы учетной функции (в правовом понимании, а также как элемента формирования страхового массива информации) и функции персональной ответственности за традиционной технологической системой с использованием учетных карточек и иных форм (описей), изготовляемыхне вручную, а автоматически — на принтере ЭВМ; автоматическая допечатка в указанные формы изменений и дополнений при движении документов;

• обязательный учет конфиденциальных электронных документов, находящихся на всех магнитных носителях и в машинных массивах, постоянная проверка службой КД реального наличия этих документов на носителях и в массивах, их целостности, комплектности и отсутствия несанкционированных копий;

• необходимость исключения технической возможности копирования информации, содержащейся в компьютере (рабочей станции) пользователя, на другие магнитные носители и работы компьютера в комплекте с принтером (изъятие из ЭВМ дисководов и т.п.);

• жесткое соблюдение персоналом правил работы с конфиденциальной электронной информацией, в частности правила, которое гласит, что все операции с информацией в компьютере должны быть письменно санкционированы полномочным должностным лицом, подотчетны службе КД и протоколироваться в машинном журнале; протоколы подлежат регулярному контролю и анализу специалистами службы КД или службы безопасности;

• изъятие конфиденциальной информации из базы данных компьютера (рабочей станции) по окончании работы с ней (например, в конце рабочего дня, при длительных перерывах в работе и т.п.) и перенос информации на дискеты, подлежащие сдаче в службу КД.

Рассмотрение и исполнение электронных конфиденциальных документов и электронных аналогов бумажных документов разрешается только при наличии сертифицированной системы защиты компьютеров и локальной сети, включающей комплекс программно-аппаратных, криптографических и технических мер защиты базы данных, компьютеров и линий связи. Помещения, в которых конфиденциальная информация обрабатывается на ЭВМ, должны иметь защиту от технических средств промышленного шпионажа, надежную круглосуточную охрану и пропускной режим. Кроме того, следует учитывать, что при автоматизированной обработке объективно резко увеличивается количество носителей (источников), содержащих конфиденциальные сведения: традиционный бумажный документ, разнообразные машинограммы карточек, описей документов, многочисленные записи информации на магнитных носителях и визуальная информация на экране дисплея. Недостатком обработки информации на ЭВМ является также необходимость постоянного дублирования информации на нескольких носителях с целью исключения опасности ее утраты или искаженияпо техническим причинам.

3. Служба КД может включать с себя следующие функциональные группы (участки деятельности):

• группу учета поступивших документов;

• группу учета носителей конфиденциальной информации;

• группу учета и обработки изданных документов;

• группу учета номенклатурных дел — архив фирмы;

• группу инвентарного учета документов;
• бюро изготовления документов;
• копировально-множительную группу;
• контрольно-методическую группу.

Тема 9. Защищенный документооборот

План:

1. Информационная безопасность электронного документооборота . Взаимоотношение ДОУ и ИТ
2. Организация документооборота
3. Разрешительная система доступа к конфиденциальным документам

1.Защита электронного документооборота от несанкционированного доступа стала одной из главных проблем, находящихся на сегодняшний день в сфере бизнеса. В связи с этим можно выделить **три группы проблем**, которые возникают при обеспечении информационной безопасности электронного документооборота:

✓ **Трудности, связанные с недостаточной поддержкой государством внедрения систем электронного документооборота (СЭД)**. Пока государство и суды не признают электронные документы, бизнес может использовать СЭД только для поддержки оперативной деятельности. Хотя с недавнего времени на некоторых предприятиях стала активно внедряться электронно-цифровая подпись (ЭЦП). Но она применяется далеко не на всех предприятиях и государством более признаются «бумажные» документы», т.е. данная отрасль является неразвитой.

✓ **Отсутствие нормативной базы, необходимой для полноценного использования электронных документов.** Так, не установлен порядок признания юридической силы электронных документов государственными органами и судами; отсутствует официально признаваемая методика работы с электронными документами, обеспечивающая признание их юридической силы; отсутствуют методики экспертизы ценности электронных документов, передачи их на архивное хранение, уничтожения электронных документов, работы с «грифованными» электронными документами, и т.д.

Перечисленные проблемы напрямую связаны с информационной безопасностью. Пока что электронные документы – вроде и не документы вовсе, и во многих организациях с ними поступают, как хотят. Часто отсутствует даже элементарный учёт имеющихся в организации программных средств и баз данных, а в результате электронные документы и информация либо утрачиваются, либо их становится невозможно ни найти, ни использовать. Уничтожение увольняющимися сотрудниками «своих» электронных богатств – самое обычное явление, с которым невозможно бороться.

✓ **Сохранение аутентичности и целостности электронных документов.** На сегодняшний день электронные документы мало признаются судами – отсюда следует вывод: если сегодня не начать архивировать электронные документы в строгом соответствии с известными международными стандартами, то завтра, когда электронные документы будут признаны на деле, организация не сможет доказать подлинность своих документов. Для компаний, ведущих международную деятельность, это уже «горящая» проблема, поскольку, к примеру, в большинстве развитых стран сообщения электронной почты признаются деловыми документами и могут быть предъявлены в качестве доказательства в суде.

Проблема обеспечения аутентичности электронных документов особенно обостряется, если их нужно хранить долго – более 5-7 лет. В этом случае, вследствие устаревания компьютерных систем и/или форматов данных, может потребоваться перенос документов в другую компьютерную систему и/или преобразование в новые форматы. Более того, каждый шаг переноса документов и преобразование из в новые форматы должен быть тщательно задокументирован для того, чтобы аутентичность документов не могла быть подвергнута сомнению.

Но даже при обычном сканировании документов для помещения их в электронный архив требуется не только документировать все действия и обеспечить техническую защиту полученных

образов документов, но и избегать операций, которые могут поставить аутентичность документов под сомнение.

Взаимоотношение ДОУ и ИТ

При внедрении систем электронного документооборота на уровне отдельной организации особую остроту приобретает проблема взаимоотношений и взаимопонимания между службой ИТ с одной стороны, и службой ДОУ, юридическим отделом и деловыми подразделениями – с другой.

Прежде всего, это проблема «делового статуса». ИТ-специалисты стоят на более высокой ступени в иерархии организации, имеют большую зарплату, пользуются гораздо большим влиянием на руководство. В коммерческих структурах денег на развитие современных технологий не жалеют, в то время как отделы ДОУ получают средства на свое развитие по остаточному принципу. Кроме того, специалисты ДОУ жалуются на то, что служба ИТ определяет требования к управлению документами, не консультируется с ДОУ при выборе и закупке систем электронного документооборота.

Именно продолжающееся внедрение информационных технологий в процесс документооборота, в сочетании с усиливающимся давлением со стороны законодательства и контролирующих органов, потихоньку приводит к изменению положения ДОУ в лучшую сторону – поскольку ряд знаний и навыков, обычных для сотрудников нашей службы и остро необходимых сейчас в электронном документообороте, не распространены среди специалистов ИТ.

К ним относятся:

1. Понимание жизненного цикла документа, который может включать такие стадии, как создание, временное хранение в соответствии с требованиями законодательства и контролирующих инстанций, экспертизу ценности, постоянное хранение или уничтожение в установленном порядке;
2. Понимание того, что вся информация организации должна управляться по единым правилам;
3. Привычка веси строгий учёт документов, их выдачи и возврата;
4. В отличие от большинства программистов, сотрудники ДОУ вынуждены продумывать свою работу как минимум на пять лет вперёд (столько времени, по закону, должны храниться документы бухгалтерского учёта). Они понимают, что нужно не просто сохранить соответствующие электронные документы, но сохранить их так, чтобы их целостность и аутентичность могла быть доказана.

Именно специалисты службы ДОУ лучше других видят проблемы, возникающие при внедрении. Особенное беспокойство вызвало то, что сотрудники ИТ и деловых подразделений плохо понимают роль электронного документооборота в обеспечении соответствия деятельности организации законодательству и нормативным требованиям.

Для успешного внедрения электронных систем и их надёжной защиты необходимо тесное сотрудничество специалистов ИТ, ДОУ и других заинтересованных сторон: деловых подразделений, юридической службы, службы информационной безопасности.

2. Установление порядка движения документов или управление документацией организации заключается в создании условий, обеспечивающих хранение необходимой документной информации, ее быстрый поиск и снабжение ею потребителей в установленные сроки и с наименьшими затратами. Она включает:

- организацию документооборота;
- создание информационно-поисковых систем по документам;
- контроль их исполнения;
- подготовку документов к передаче на архивное хранение.

По определению "Движение документов с момента их получения или создания до завершения исполнения, отправки адресату или сдачи на хранение" образует документооборот. Соответственно масштабам движения документов можно выделить документооборот конкретного должностного лица, структурного подразделения, организации, отрасли управления, государства в целом.

Действующие нормативные акты и методические документы, в том числе и «Государственная система документационного обеспечения управления. Основные положения. Общие требования к документам и службам документационного обеспечения» (ГСДОУ), исходя из прагматических соображений, рассматривают в качестве объекта регулирования только документооборот организации в целом и соответственно потоки входящих, внутренних и исходящих документов.

ГСДОУ требует закрепления порядка движения документов внутри организаций в схемах, разрабатываемых службой делопроизводства и утверждаемых руководством организаций. В подобные схемы должны быть включены все, в том числе и компьютерные пункты обработки документной информации и, если они поддаются нормированию, сроки прохождения и обработки документов. Самостоятельные схемы разрабатываются для различных категорий документов: входящих, исходящих, внутренних, приказов по личному составу и по основной деятельности и т.д. В эти схемы включаются, как правило, этапы создания документов от момента написания черновика. В случае утверждения схем движения документов руководством организации они приобретают нормативную силу.

Документооборот, или порядок движения документов в организации, можно разделить на следующие ***этапы***:

1. Экспедиционная обработка документов, поступающих в организацию.
2. Предварительное рассмотрение документов службой документационного обеспечения.
3. Рациональное движение документов внутри организации.
4. Обработка исполненных и отправляемых документов.

Организация конфиденциального делопроизводства

Правильная организация конфиденциального делопроизводства в фирме является составной частью комплексного обеспечения безопасности информации и имеет важное значение в достижении цели ее защиты. Как известно, специалисты, занимающиеся в области информационной безопасности утверждают, что порядка 80% конфиденциальной информации находится в документах делопроизводства. Поэтому вопросы конфиденциального документооборота в фирме несомненно играют важную роль в достижении ею экономических успехов. В данной статье даны некоторые рекомендации, позволяющие упорядочить работу в фирме с конфиденциальными документами.

Всю информацию в фирме (организации) можно разделить на две большие группы:

- открытую;
- с ограниченным доступом.

В свою очередь ***информация с ограниченным доступом*** может быть:

- ✓ государственной тайной;
- ✓ конфиденциальной информацией.

А, следовательно, и ***документы***, содержащие ту или иную информацию подразделяются на ***секретные и конфиденциальные***. *Причем, секретные документы могут быть* ***с грифом "Секретно", "Совершенно секретно", "Особой важности".*** *Конфиденциальные документы соответственно* ***с грифами "Коммерческая тайна"*** и т.д.

В настоящее время видов конфиденциальной информации (а, следовательно, и возможных грифованных документов) насчитывается более 30. Что в целом не создает благоприятной атмосферы в смысле обеспечения их безопасности. По этой причине количество видов конфиденциальной информации в перспективе, надо полагать, уменьшится. Каждый вид конфиденциальных документов имеет реквизиты.

По своей природе конфиденциальные документы бывают:

- нормативно-методические;
- руководящие;
- распорядительные;
- информационно-справочные;
- организационные;
- финансово-бухгалтерские;
- кадровые (по личному составу).

Конфиденциальные документы должны обрабатываться в конфиденциальном делопроизводстве фирмы, либо в общем делопроизводстве, специально назначенным должностным лицом, ответственным за конфиденциальные документы. Конфиденциальные документы должны храниться в отдельном помещении в запираемых и опечатываемых шкафах. Допускается хранение конфиденциальных документов в общем делопроизводстве. Но обязательно они должны находиться отдельно от других дел делопроизводства.

В зависимости от назначения ***конфиденциальные документы подразделяются на:***

- входящие;
- исходящие;
- внутренние.

Прием входящих конфиденциальных документов осуществляется сотрудником конфиденциального делопроизводства.

При этом проверяется:

- количество листов;
- количество экземпляров;
- наличие приложений (если они указаны в сопроводительном письме).

В случае отсутствия в пакете (конверте) некоторых перечисленных документов - составляется акт в 2-х экземплярах. Один экземпляр акта отправляется в адрес отправителя.

Регистрация документов производится в электронной базе, в журналах регистрации, либо на карточках.

На каждом зарегистрированном документе должен проставляться штамп, в котором указывается:

- наименование;
- регистрационный номер;
- дата поступления.

После регистрации документы передаются руководству организации для принятия решения. Руководитель после рассмотрения документа определяет исполнителя и дает указания по исполнению документа. Эти указания оформляются на самом документе в виде резолюции.

С резолюцией руководителя конфиденциальный документ передается исполнителю под расписку в журнале регистрации входящих конфиденциальных документов.

По завершении работы над документом на нем проставляется отметка о его исполнении и направлении в дело. После чего документ сотрудником конфиденциального делопроизводства подшивается в дело.

Все дела с конфиденциальными документами и журналы их учета вносятся в номенклатуру дел организации.

По окончании каждого года руководителем организации создается комиссия, которая должна:

- проверить наличие конфиденциальных документов;
- определить конфиденциальные документы для архивного хранения;
- определить конфиденциальные документы, подлежащие уничтожению.

В случае утери конфиденциального документа руководителем организации создается комиссия, которая проводит расследование по факту утраты данного документа. По результатам работы комиссии руководителем организации принимается решение о привлечении к ответственности лиц виновных в утрате конфиденциального документа.

Принципы защиты конфиденциального документооборота

Организация конфиденциального документооборота должна строиться на основе следующих **принципов**:

- Разрешительной системы доступа к конфиденциальным документам;
- Обеспечения пользователей всеми необходимыми им в силу служебных обязанностей конфиденциальными документами, но только теми, которые действительно необходимы для выполнения конкретных видов работы;
- Исключения несанкционированного доступа к конфиденциальным документам;

- Целенаправленного регулирования процессов движения конфиденциальных документов;
- Исключения инстанций прохождения конфиденциальных документов и действий с ними, не обусловленных характером и порядком исполнения документов;
- Фиксированной передачи конфиденциальных документов;
- Обеспечения своевременного и качественного исполнения конфиденциальных документов;
- Персональной и обязательной ответственности за выдачу неправомерных разрешений и ознакомление с конфиденциальными документами и на их отправление.

Как и многие другие задачи, проблема защиты конфиденциального документооборота решается только в том случае, когда служба ДОУ, отвечающая главным образом за «бумажную» работу, и служба информационных технологий, контролирующая сегодня электронные документы и материалы, объединяются в единое целое и действуют совместно.

3. Разрешительная система доступа к конфиденциальным документам представляет собой совокупность установленных руководством предприятия нормативных положений, обеспечивающих обоснованный и правомерный доступ пользователей к необходимому им для выполнения служебных обязанностей объему конфиденциальных документов. Системой должно быть определено, кто из руководителей предприятия и структурных подразделений, кому из пользователей и с какими категориями конфиденциальных документов может давать разрешение на ознакомление (работу), а также порядок оформления таких разрешений в зависимости от вида учета или категорий документов. При этом право давать разрешение на ознакомление и право работать с конфиденциальными документами может быть предоставлено только лицам, имеющим допуск к коммерческой тайне.

При установлении разрешительной системы доступа к конфиденциальным документам необходимо учитывать следующие требования:

- соответствующий руководитель может давать разрешение на ознакомление с конфиденциальными документами, входящими в сферу его деятельности. Только подчиненным лицам и только по служебной необходимости;
- разрешение на ознакомление оформляется письменно;
- при необходимости ознакомления пользователя только с частью конфиденциального документа в разрешении на ознакомление должны быть указаны разделы, пункты или страницы, с которыми можно знакомить пользователя.

Разрешительная система должна предусматривать и порядок доступа к конфиденциальным документам лиц, не работающих на данном предприятии (при выполнении совместных работ и др.). За разглашение или неправомерное использование содержащихся в документах конфиденциальной информации сотрудники, получившие доступ к конфиденциальным документам несут перед обладателем этих документов гражданско-правовую ответственность.

Защищенность документопотоков достигается за счет:

- одновременного использования режимных (разрешительных, ограниченных) мер и технологических приемов, входящих в систему обработки и хранения конфиденциальных документов;
- нанесения отличительной отметки (грифа) на чистый носитель конфиденциальной информации или документ, в том числе сопроводительный, что позволяет выделить их в общем потоке документов;
- формирования самостоятельных, изолированных потоков конфиденциальных документов и часто дополнительного их разбиения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;
- использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающихся с системой обработки открытых документов;
- регламентации движения документов как внутри фирмы, так и между фирмами, т.е. с момента возникновения мысли о необходимости создания документа и до окончания работы с документом и передачи его в архив;

- организации самостоятельного подразделения конфиденциальной документации или аналогичного подразделения, входящего (или не входящего) в состав службы безопасности или аналитической службы;

перемещения документов между руководителями, исполнителями и иным персоналом только через службу конфиденциального делопроизводства.

Методические рекомендации (указания) к практическим занятиям

Важной составной частью учебного процесса являются практические занятия.

Задачей преподавателя при проведении практических работ является грамотное и доступное разъяснение принципов и правил проведения работ, побуждение обучающихся к самостоятельной работе, определения места изучаемой дисциплины в дальнейшей профессиональной работе будущего выпускника.

Практическое занятие - форма организации обучения, когда обучающиеся по заданию и под руководством преподавателя выполняют одну или несколько практических работ.

Основные дидактические цели практических работ - экспериментальное подтверждение изученных теоретических положений. В ходе работы обучающиеся вырабатывают умения наблюдать, сравнивать, сопоставлять, анализировать, делать выводы и обобщения, самостоятельно вести исследования.

Организация и проведение практических работ.

Выполнение обучающимися практических работ направлено:

- на обобщение, систематизацию, углубление и закрепления полученных теоретических знаний;

- на формирование умений применять полученные знания на практике;

- на выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Практическая работа, как вид учебного занятия проводиться в учебных кабинетах.

Продолжительность - не менее двух академических часов. Необходимыми структурными элементами практической работы являются:

- самостоятельная деятельности студентов,

- инструктаж, проводимый преподавателем,

- организация обсуждения итогов выполнения практической работы.

Перед началом выполнения практической работы проводится проверка знаний обучающихся - их теоретической готовности к выполнению задания.

Форма организации обучающихся на практических работах - индивидуальная.

При индивидуальной форме организации занятий каждый обучающийся выполняет индивидуальное задание.

Оформление практических работ

Практическая работы по дисциплине оформляется в тетради

Структура работы:

- тема, цель работы,

- основная часть (описание ситуации, задачи)

- выводы.

Оценки за выполнение практических работ выставляться по пятибалльной системе или в форме зачета и учитываться как показатели текущей успеваемости обучающихся.

Если по практической работе выставляется зачет, то итоговая оценка выставляется по итоговой работе (итоговая письменная контрольная работа, итоговая практическая работа).

Методические рекомендации по работе с ситуационными заданиями и кейсами

Решение кейса представляет собой продукт самостоятельной индивидуальной или групповой работы студентов. Работа с кейсом осуществляется поэтапно: Первый этап – знакомство с текстом кейса, изложенной в нем ситуацией, ее особенностями. Второй этап – выявление фактов, указывающих на проблему(ы), выделение основной проблемы (основных проблем), выделение факторов и персоналий, которые могут реально воздействовать. Третий этап – выстраивание иерархии про-

блем (выделение главной и второстепенных), выбор проблемы, которую необходимо будет решить. Четвертый этап – генерация вариантов решения проблемы. Возможно проведение «мозгового штурма». Пятый этап – оценка каждого альтернативного решения и анализ последствий принятия того или иного решения. Шестой этап – принятие окончательного решения по кейсу, например, перечня действий или последовательности действий. Седьмой этап – презентация индивидуальных или групповых решений и общее обсуждение. Восьмой этап - подведение итогов в учебной группе под руководством

Рекомендации по осуществлению анализа кейс-задания

Ознакомление студентов с текстом кейса и последующий анализ кейса может осуществляться заранее (за несколько дней до его обсуждения) как самостоятельная работа студентов. Общая схема работы с кейсом на этапе анализа может быть представлена следующим образом: в первую очередь следует выявить ключевые проблемы кейса и понять, какие именно из представленных данных важны для решения; войти в ситуационный контекст кейса, определить, кто его главные действующие лица, отобрать информацию необходимую для анализа, понять, какие трудности могут возникнуть при решении задачи.

Для успешного анализа кейсов следует придерживаться ряда принципов:

используйте знания, полученные в процессе лекционного курса; внимательно читайте кейс для ознакомления с имеющейся информацией, не торопитесь с выводами; не смешивайте предположения с фактами; При проведении письменного анализа кейса помните, что основное требование, предъявляемое к нему, – краткость.

Презентация результатов анализа кейсов

Презентация, или представление результатов анализа кейса, выступает очень важным элементом метода. При этом в case-study используются два вида презентаций: устная (публичная) и письменный отчет-презентация. Публичная (устная) презентация предполагает представление решений кейса группе. Устная презентация требует навыков публичного выступления, умения кратко, но четко и полно изложить информацию, убедительно обосновать предлагаемое решение, корректно отвечать на критику и возражения. Подготовка письменного анализа кейса аналогична подготовке устного, с той разницей, что письменные отчеты-презентации обычно более структурированы и детализированы. Основное правило письменного анализа кейса заключается в том, чтобы избегать простого повторения информации из текста, информация должна быть представлена в переработанном виде. Самым важным при этом является собственный анализ представленного материала, его соответствующая интерпретация и сделанные предложения. Письменный отчет – презентация может сдаваться по истечении некоторого времени после устной презентации, что позволяет более тщательно проанализировать всю информацию, полученную в ходе дискуссии.

Оценка за кейс-задание выставляется по четырѐхбалльной шкале.

«Отлично» – кейс–задание выполнено полностью, в рамках регламента, установленного на публичную презентацию, студент(ы) приводит (подготовили) полную четкую аргументацию выбранного решения на основе качественно сделанного анализа. Демонстрируются хорошие теоретические знания, имеется собственная обоснованная точка зрения на проблему(ы) и причины ее (их) возникновения. В случае ряда выявленных проблем четко определяет их иерархию. При устной презентации уверенно и быстро отвечает на заданные вопросы, выступление сопровождается приемами визуализации. В случае письменного отчета-презентации по выполнению кейс-задания сделан структурированный и детализированный анализ кейса, представлены возможные варианты решения (3-5), четко и аргументировано обоснован окончательный выбор одного из альтернативных решений.

«Хорошо» – кейс–задание выполнено полностью, но в рамках установленного на выступление регламента, студент(ы) не приводит (не подготовили) полную четкую аргументацию выбранного решения. Имеет место излишнее теоретизирование, или наоборот, теоретическое обоснование ограничено, имеется собственная точка зрения на проблемы, но не все причины ее возникновения установлены. При устной презентации на дополнительные вопросы выступающий отвечает с некоторым затруднением, 14 подготовленная устная презентации выполненного кейс-задания не

очень структурирована. При письменном отчете-презентации по выполнению кейсзадания сделан не полный анализ кейса, без учета ряда фактов, выявлены не все возможные проблемы, для решения могла быть выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 2-3, затруднена четкая аргументация окончательного выбора одного из альтернативных решений

«Удовлетворительно» – кейс–задание выполнено более чем на 2/3, но в рамках установленного на выступление регламента, студент(ы) расплывчато раскрывает решение, не может четко аргументировать сделанный выбор, показывает явный недостаток теоретических знаний. Выводы слабые, свидетельствуют о недостаточном анализе фактов, в основе решения может иметь место интерпретация фактов или предположения, Собственная точка зрения на причины возникновения проблемы не обоснована или отсутствует. При устной презентации на вопросы отвечает с трудом или не отвечает совсем. Подготовленная презентация выполненного кейс-задания не структурирована. В случае письменной презентации по выполнению кейс-задания не сделан детальный анализ кейса, далеко не все факты учтены, для решения выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 1-2, отсутствует четкая аргументация окончательного выбора решения.

«Неудовлетворительно» – кейс-задание не выполнено, или выполнено менее чем на треть. Отсутствует детализация при анализ кейса, изложение устное или письменное не структурировано. Если решение и обозначено в выступлении или отчете-презентации, то оно не является решением проблемы, которая заложена в кейсе.

Методические указания для самостоятельной работы студентов

Самостоятельная работа студентов – важнейшая составная часть учебного процесса, обязательная для каждого студента, объем которой определяется учебным планом. Методологическую основу СРС составляет деятельностный подход, при котором цели обучения ориентированы на формирование умений решать типовые и нетиповые задачи, т. е. на реальные ситуации, в которых студентам надо проявить знание конкретной дисциплины.

Планируемые результаты организации самостоятельной работы студентов предполагают: усвоение знаний, формирование профессиональных умений, навыков и компетенций будущего специалиста; закрепление знания теоретического материала практическим путем; воспитание потребности в самообразовании; максимальное развитие познавательных и творческих способностей личности; побуждение к научно-исследовательской работе; повышение качества и интенсификации образовательного процесса; формирование интереса к избранной профессии и овладению ее особенностями; осуществление дифференцированного подхода в обучении. применение полученных знаний и практических навыков для анализа ситуации и выработки правильного решения, для формирования собственной позиции, теории, модели.

Составление опорного конспекта (подготовка к практическому занятию)

Представляет собой вид внеаудиторной самостоятельной работы студента по созданию краткой информационной структуры, обобщающей и отражающей суть материала лекции, темы учебника. Опорный конспект призван выделить главные объекты изучения, дать им краткую характеристику, используя символы, отразить связь с другими элементами. Основная цель опорного конспекта – облегчить запоминание. В его составлении используются различные базовые понятия, термины, знаки (символы) – опорные сигналы. Опорный конспект – это наилучшая форма подготовки к ответу и в процессе ответа. Опорный конспект может быть представлен системой взаимосвязанных геометрических фигур, содержащих блоки концентрированной информации в виде ступенек логической лестницы; рисунка с дополнительными элементами и др. Роль студента: изучить материалы темы, выбрать главное и второстепенное; установить логическую связь между элементами темы; представить характеристику элементов в краткой форме; выбрать опорные сигналы для акцентирования главной информации и отобразить в структуре работы; оформить работу и предоставить в установленный срок.

Критерии оценки: соответствие содержания теме; правильная структурированность информации; наличие логической связи изложенной информации; соответствие оформления требованиям; аккуратность и грамотность изложения; работа сдана в срок.

Написание реферата

Это более объемный, чем сообщение, вид самостоятельной работы студента, содержащий информацию, дополняющую и развивающую основную тему, изучаемую на аудиторных занятиях. Ведущее место занимают темы, представляющие профессиональный интерес, несущие элемент новизны. Реферативные материалы представляют письменную модель первичного документа – научной работы, монографии, статьи. Реферат может включать обзор нескольких источников и служить основой для доклада на определенную тему на практическом занятии Регламент озвучивания реферата – 7-10 мин.

При подготовке реферата необходимо соблюдать следующие правила. Определить идею и задачу реферата. Ясно и четко сформулировать тему или проблему. Она не должна быть слишком общей. Найти нужную литературу по выбранной теме. Составить перечень литературы, которая обязательно должна быть прочитана. Только после предварительной подготовки следует приступать к написанию реферата. Прежде всего, составить план, выделить в нем части. Введение, в котором раскрывается цель и задачи сообщения; здесь необходимо сформулировать социальную или политическую проблему которая будет проанализирована в реферате, изложить своё отношение к ней, то есть мотивацию выбора; определить особенность постановки данной проблемы авторами изученной литературы; объяснить актуальность и социальную значимость выбранной темы. Основная часть. Разделы, главы, параграфы основной части должны быть направлены на рассмотрение узловых моментов в теме реферата. Изложение содержания изученной литературы предполагает его критическое осмысление, глубокий логический анализ. Каждый раздел основной части реферата предполагает детальное изучение отдельного вопроса темы и последовательное изложение структуры текстового материала с обязательными ссылками на первоисточник. В целом, содержание основной части должно отражать позиции отдельных авторов, сравнительную характеристику этих позиций, выделение узловых вопросов дискурса по выбранной для исследования теме.

Для лучшего изложения сущности анализируемого материала можно проиллюстрировать его таблицами, графиками, сравнением цифр, цитатами. Заключение. В заключении автор реферата должен сформулировать личную позицию в отношении изученной проблемы и предложить, может быть, свои способы её решения. Целесообразно сделать общие выводы по теме реферата и ещё раз отметить её актуальность и социальную значимость Начать реферат можно с изложения яркого, впечатляющего факта, который требует пояснения. Далее изложение должно идти от простого – к сложному. Не останавливайтесь на подробностях. Главное требование к реферату – максимум пользы для читателя при минимуме информации. Написание рефератов является одной из форм обучения студентов, направленных на организацию и повышение уровня самостоятельной работы студентов, а также на усиление контроля за этой работой. Целью написания рефератов является привитие студентам навыков самостоятельной работы с литературой с тем, чтобы на основе их анализа и обобщения студенты могли делать собственные выводы теоретического и практического характера, обосновывая их соответствующим образом. В отличие от теоретических семинаров, при проведении которых студент приобретает, в частности, навыки высказывания своих суждений и изложения мнений других авторов в устной форме, написание рефератов даст ему навыки лучше делать то же самое, но уже в письменной форме, грамотным языком и в хорошем стиле. Представляется, что в зависимости от содержания и назначения в учебном процессе рефераты можно подразделить на две основные группы (типы): научно-проблемные и обзорно-информационные. Научно-проблемный реферат.

Написание реферата и его защита перед преподавателем или группой предполагает, что студент должен знать правила написания и оформления реферата, а также уметь подготовить сообщение по теме своего реферата, быть готовым отвечать на вопросы преподавателя и студентов по содержанию реферата.

Методические рекомендации по составлению информационных сообщений (докладов)

Информационное сообщение (доклад) – есть результат процессов преобразования формы и содержания документов с целью их изучения, извлечения необходимых сведений, а также их оценки, сопоставления, обобщения и представления в устной форме (защиты)

Требования к оформлению

Объем информационных сообщений (докладов) – до 5 полных страниц текста, набранного в текстовом редакторе Word, шрифтом – TimesNewRoman, 14 шрифтом с одинарным межстрочным интервалом, параметры страницы – поля со всех сторон по 20 мм.

Ссылки на литературу концевые, 10 шрифтом. В названии следует использовать заглавные буквы, полужирный шрифт, при этом не следует использовать переносы; выравнивание осуществлять по центру страницы. Данные об авторе указываются 14 шрифтом (курсивом) в правом верхнем углу листа.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература:

1. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 186 c. — 5-89838-138-4. — Режим доступа: http://www.iprbookshop.ru/7008.html.
2. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электронный ресурс] : учебник / Н.Н. Куняев [и др.]. — Электрон. текстовые данные. — М. : Логос, 2016. — 500 c. — 978-5-98704-711-8. — Режим доступа: http://www.iprbookshop.ru/66416.html.

б) дополнительная литература:

3. Кришталюк А.Н. Конфиденциальное делопроизводство и защита коммерческой тайны [Электронный ресурс] : курс лекций / А.Н. Кришталюк. — Электрон. текстовые данные. — Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 199 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/33427.html.
4. Аверченков В.И. Организационная защита информации [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 184 c. — 978-89838-489-0. — Режим доступа: http://www.iprbookshop.ru/7002.html.
5. Минин О.В. Защита конфиденциальной информации при электронном документообороте [Электронный ресурс] : учебное пособие / О.В. Минин, И.В. Минин. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2011. — 20 c. — 978-5-7782-1829-1. — Режим доступа: http://www.iprbookshop.ru/44918.html.
6. Северин В.А. Коммерческая тайна в России [Электронный ресурс] : монография / В.А. Северин. — Электрон. текстовые данные. — М. : Зерцало-М, 2009. — 472 c. — 978-5-94373-163-1. — Режим доступа: http://www.iprbookshop.ru/4030.html.
7. Беловицкий К.Б. Режим коммерческой тайны в системе обеспечения экономической безопасности хозяйствующего субъекта [Электронный ресурс] : учебное пособие / К.Б. Беловицкий. — Электрон. текстовые данные. — М. : Научный консультант, 2017. — 124 c. — 978-5-9909964-4-1. — Режим доступа: http://www.iprbookshop.ru/75143.html.