2. Конспект лекций

Тема 1 Введение. Основные понятия, связанные с функционированием службы защиты информации

Защита информации (ЗИ) — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных) [4, 9].

Некоторые определения. Система называется безопасной, если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

Очевидно, что абсолютно безопасных систем нет, и здесь речь идет о надежной (доверенной) системе, т. е. «системе, которой можно доверять» (как можно доверять человеку). Система считается надежной, если она с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Основными критериями оценки надежности являются: политика безопасности и гарантированность.

Политика безопасности, являясь активным компонентом зашиты (включает в себя анализ возможных угроз и выбор соответствующих мер противодействия), отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации.

Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии со сформулированной политикой безопасности.

Гарантированность, являясь пассивным элементом зашиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).

В надежной системе должны регистрироваться все происходящие события, касающиеся безопасности (должен использоваться механизм подотчетности протоколирования, дополняющийся анализом запомненной информации, т. е. аудитом).

При оценке степени гарантированности, с которой систему можно считать надежной, центральное место занимает достоверная (надежная) вычислительная база. Достоверная (доверенная, надежная) вычислительная база (ДВБ, или ТСВ — Trusted Computer Base) представляет собой полную совокупность защитных механизмов компьютерной системы, которая используется для претворения в жизнь соответствующей политики безопасности.

Надежность ДВБ зависит исключительно от ее реализации и корректности введенных данных (например, данных о благонадежности пользователей, определяемых администрацией).

Граница ДВБ образует периметр безопасности. Компоненты ДВБ, находящиеся внутри этой границы, должны быть надежными (следовательно, для оценки надежности компьютерной системы достаточно рассмотреть только ее ДВБ). От компонентов, находящихся вне периметра безопасности, вообще говоря, не требуется надежности. Однако это не должно влиять на безопасность системы, так как сейчас более широко применяются распределенные системы обработки данных, то под «периметром безопасности» понимается граница владений определенной организации, в подчинении которой находится эта система. Тогда по аналогии то, что находится внутри этой границы, считается надежным. Посредством шлюзовой системы, которая способна противостоять потенциально ненадежному. а может быть даже и враждебному окружению, осуществляется связь через эту границу.

Контроль допустимости выполнения субъектами определенных операций над объектами, т. е. функции мониторинга, выполняется достоверной вычислительной базой. При каждом обращении пользователя к программам или данным монитор проверяет допустимость

данного обращения (согласованность действия конкретного пользователя со списком разрешенных для него действий). Реализация монитора обращений называется ядром безопасности, на базе которой строятся все защитные механизмы системы. Ядро безопасности должно гарантировать собственную неизменность.

Предметная область «Защита информации» согласно ГОСТ Р 50922—96 [1|. Основополагающим здесь является понятие «защита информации» с позиции собственника, владельца, пользователя информацией как деятельность (процесс), направленная на предотвращение утечки защищаемой информации, а также по предотвращению различного рода несанкционированных воздействий (НСВ) на информацию и се носители, т. с. защита информации от угроз безопасности информации. Могут быть также введены более узкие области (рис. 1.1):

- защита информации от разглашения;
- защита информации от утечки по каналам (иностранной) технической разведки.
- защита информации от физического (частного) лица;
- защита информации от несанкционированного доступа;
- защита информации от несанкционированных воздействий, которые, в свою очередь, могут включать такие разделы предметной области, как:
  - защита информации от утечки по каналам радио-, радиотехнической разведки;

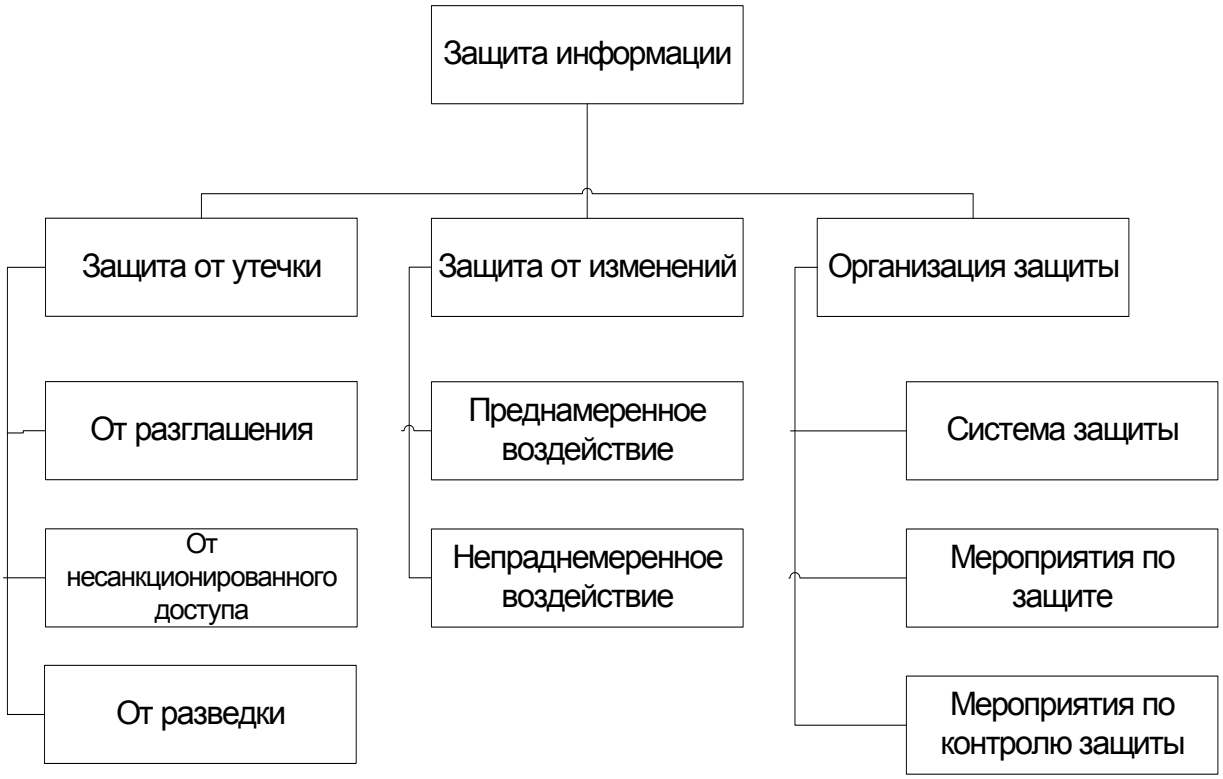

Рис. 1.1. Структура предметной области «Зашита информации» согласно ГОСТ Р50922 96

- защита информации от утечки по каналам визуально-оптической разведки;
- защита информации от утечки по акустическому каналу;
- защита информации от утечки за счет побочных электромагнитных излучений и наволок (ПЭМИН);
- защита информации от утечки по каналам специальных электронных закладных устройств;
- защита информации от несанкционированного доступа (НСД) при ее обработке с помощью технических средств (средств вычислительной техники и средствах связи, в средствах оргтехники);

— защита информации шифрованием:
— защита информации режимно-секретной деятельностью;
— защита информации обеспечением безопасности связи.

Основные предметные направления ЗИ

Основные предметные направления ЗИ — охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности [14].

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Сведения могут считаться государственной тайной (могут быть засекречены), если они отвечают следующим требованиям:

– соответствуют перечню сведений, составляющих государственную тайну, не входят в перечень сведений, не подлежащих засекречиванию, и отвечают законодательству РФ о государственной тайне (принцип законности);

– целесообразность засекречивания конкретных сведений установлена путем экспертной опенки вероятных экономических и иных последствий, возможности нанесения ущерба безопасности РФ, исходя из баланса жизненно важных интересов государства, общества и личности (принцип обоснованности);

– ограничения на распространение этих сведений и на доступ к ним установлены с момента их получения (разработки) или заблаговременно (принцип своевременности):

– компетентные органы и их должностные лица приняли в отношении конкретных сведений решение об отнесении их к государственной тайне и засекречивании и установили в отношении их соответствующий режим правовой охраны и защиты (принцип обязательной зашиты).

Коммерческая тайна исстари охранялась при содействии государства. Примером этого утверждения могут служить многочисленные факты ограничения доступа иностранцев в страну (в Китае — для защиты секретов производства фарфора), в отдельные отрасли экономики или на конкретные производства. В России к коммерческой тайне относили промысловую тайну, но затем она была ликвидирована как правовой институт в начале 30-х годов и в связи с огосударствлением отраслей экономики защищалась как государственная и служебная тайна. Сейчас начался обратный процесс.

Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

– имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам;

– не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;

– к ней нет свободного доступа на законном основании;

– обладатель информации принимает меры к охране ее конфиденциальности.

Основными субъектами права на коммерческую тайну являются обладатели коммерческой тайны, их правопреемники.

Обладатели коммерческой тайны — физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

При этом под предпринимательством понимается «самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке» (ст. 2 Гражданского кодекса Российской Федерации).

Правопреемники — физические и юридические лица, которым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна информация, составляющая коммерческую тайну другого лица.

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

Профессиональная тайна — защищаемая по закону информация. доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

– доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей:

– лицо, которому доверена информация, не состоит на государственной или муниципальной службе (в противном случае информация считается служебной тайной):

– запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;

– информация не относится к сведениям, составляющим государственную и коммерческую тайну.

В соответствии с этими критериями можно выделить следующие объекты профессиональной тайны: в***рачебная тайна, тайна связи***, ***нотариальная тайна***, ***адвокатская тайна, тайна усыновления***, ***тайна страхования***, ***тайна исповеди***.

Служебная тайна — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления ее правовой охраны и защиты необходим специальный федеральный закон «О служебной тайне».

Информации может считаться служебной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

– отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону иди в силу служебной необходимости (собственная служебная тайна);

– является охраноспособной конфиденциальной информацией («чужой тайной») другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна);

– не является государственной тайной и не подпадает под перечень сведений, доступ к которым не может быть ограничен;

– получена представителем государственного органа и органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом.

В действующем законодательстве приводится перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, в том числе юридических лиц, рассмотренных в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Особенность правоотношений в этой области состоит в том, что если во втором случае государственные органы и их должностные лица обязаны обеспечить (гарантировать) сохранность «чужой» тайны, ставшей известной им по службе, в объеме сведений, переданных ее владельцем, то в первом случае, они самостоятельно в соответствии с законом определяют объем своей служебной тайны и режим ее зашиты.

Охрана персональных данных. В Европе для охраны и защиты права на неприкосновенность частой жизни в условиях автоматизированной обработки личных данных о гражданах более 25 лет назад был введен особый институт правовой охраны личности — институт зашиты персональных данных. Более чем в 20 европейских государствах приняты национальные законы о персональных данных, в ряде стран введены независимые уполномоченные по защите персональных данных, во всех странах Европейскою Союза с 1998 г. создана единая унифицированная система зашиты персональных данных, в том числе в секторе телекоммуникаций.

Федеральный закон «Об информации, информатизации и защите информации» вводит понятие «персональные данные» (ст. 2); относит персональные данные к конфиденциальной информации и устанавливает, что перечни персональных данных должны быть закрещены федеральным законом (ст. 11); требует, чтобы деятельность не государственных организаций и частных лиц по обработке и предоставлению персональных данных, равно как и по проектированию, производству средств защиты информации и обработки персональных данных обязательно лицензировались в порядке, установленном Правительством Российской Федерации (ст. 11, 19); декларирует, что персональные данные должны защищаться, а режим зашиты в отношении персональных данных устанавливается федеральным законом (ст. 21).

Объектом правоотношений здесь выступает право на персональные данные — информация (зафиксированная на любом материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним.

К персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:

Субъектами права здесь выступают:

– субъекты персональных данных — лица, к которым относятся соответствующие данные, и их наследники;

– держатели персональных данных — органы государственной власти и органы местного самоуправления, юридические и физические лица, осуществляющие на законных основаниях сбор, хранение, передачу, уточнение, блокирование, обезличивание, уничтожение персональных данных (баз персональных данных).

Персональные данные и работа с ними должны соответствовать следующим требованиям:

– персональные данные должны быть получены и обработаны законным образом на основании действующего законодательства:

– персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме, за исключением случаев, прямо установленных в законе;

– персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним. Не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации;

– персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться;

– персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению по достижении этой цели или по минновании надобности;

– персональные данные охраняются в режиме конфиденциальной информации, исключающем их случайное или несанкционированное разрушение или случайную их утрату, а равно несанкционированный доступ к данным, их изменение, блокирование или передачу;

– для лиц, занимающих высшие государственные должности, и кандидатов на эти должности может быть установлен специальный правовой режим для их персональных данных, обеспечивающий открытость только общественно значимых данных.

Охрана интеллектуальной собственности. К числу основных объектов интеллектуальной собственности отнесены: произведения науки, литературы или искусства; результаты исполнительской деятельности артистов, режиссеров, дирижеров; сложные результаты творчества; звукозаписи и записи изображения; передача радио- и телевизионных сигналов; изобретения; полезные модели; промышленные образцы; профессиональные секреты (ноу хау); селекционные достижения; фирменные наименования и коммерческие обозначения правообладателя; товарные знаки и знаки обслуживания; наименования мест происхождения товаров; другие результаты интеллектуальной деятельности и средства индивидуализации, на которые в соответствии с законом могут признаваться или закрепляться исключительные права.

Способы и подходы к защите информации

Политика информационной безопасности – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Процесс ЗИ определяется принятой политикой безопасности и реализуется системой ЗИ на основе выбранных способов и средств защиты.

Система защиты информации (СЗИ) – совокупность органов по ЗИ, используемых ими способов и средств ЗИ, а также объектов защиты, организованная и функционирующая по правилам и нормам, установленными нормативно-правовыми актами в области защиты информации.

Организация ЗИ – подразделение, отдельные должности, созданные с целью обеспечения ЗИ.

Способ ЗИ – действия применяемые для ЗИ

Метод ЗИ – порядок применяемых способов СЗИ для обеспечения требований безопасности информации.

Средство ЗИ – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для ЗИ.

Объект защиты - защищаемая информация, носитель защищаемой информации или информационный процесс.

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.*Информационный процесс* – процесс сбора, обработки, накопления, также и распространение

Литература: 1,2,3,4

Тема 2 Место и роль службы защиты информации в системе защиты информации; задачи и функции службы

В развитой составляющей отечественного комплекса информационной безопасности можно выделить такие типовые организационные структуры: служба контроля, надзора, специализированные предприятия, сертификационно-испытательные центры, аттестационные центры, службы безопасности и защиты информации предприятий и организаций. [5]

Служба защиты информации (СЗИ) является самостоятельной структурным подразделением и тесно связана со службами охраны и объектового режима. СЗИ взаимодействует со всеми структурными подразделениями, составляют основу всей системы обеспечения информационной безопасности.

Деятельность по организации функционирования и эксплуатации комплексов обеспечения информационной безопасности осуществляется штатными специалистами, имеющими определенную квалификацию в соотвествии с требованиями, установленными номенклатурой должностей и служащих.

Деятельность осуществляется в рамках нескольких направлений, которые определяются потребностями реальных бизнес-процессов, их спецификой и масштабами:

1. Физическая защита информации и имущества.
2. Обеспечение безопасности передачи информации при реализации бизнес-процессов. Организациясекретного и конфиденциального делопроизводства.
3. Подготовка и обучение персовнала.
4. Мониторинг, контроль и оценка эффективности функционирования системы информационной безопасности.
5. Формирование трехуровневой структуры стратегического, тактического и оперативного управления.

Можно выделить следующие группы задач в рамках основных направлений деятельности:

Организационные задачи и функции службы защиты информации.

1. Определение целей и приоритетных направлений работы по обеспечению безопасности деятельности предприятия
2. разработка и проектов защиты для каждого вида безопасности их реализация приемки и контроль за постоянной работоспособности
3. разработка нормативных документов для всех видов безопасности с учетом их конф и контроль за их соблюдением всеми сотрудниками и клиентами
4. организация обучения персонала правилам соблюдения и поддержания безопасной деятельности предприятия
5. организация проведения совместно с другими подразделениями мероприятий в отношении конкурентов, взаимодействия с правоохранительными органами

Технологические задачи и функции службы защиты информации.

- материально-техническое и технологическое обеспечение режима без-ти на предприятии,
- освоение и использование спец. техники, содействии в освоении новых видов техники, обучение персонала,

Координационные задачи и функции службы защиты информации.

- участие СБ в расстановке кадров, выявлением негативных тенденции в трудовых коллективах, возможных причин и условий соц. напряженности,
- оказание управленческих воздействий на создание/поддержку своевременной реорганизацию структуры управления без-ти предприятия,
- взаимодействия и координации между отдельными звеньями (отделами, группами) для достижения целей безопасности.

Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы защиты информации.

Служба защиты информации является составной частью системы защиты, является органом управления защитой информации, координирует и организует деятельность по обеспечению безопасности информации в организации в том числе с использованием технических средств и организационных мер.

Факторы: финансовые возможности предприятия, масштабы предприятия, его географическое расположение и распределенность, виды обрабатываемой информации, вид деятельности предприятия, наличие посторонних, посетителей.

Управленческая деятельность в области защиты информации.

В качестве функций управления подразделением по ЗИ выступают такие функции как (рис. 2.1): планирование; организация; мотивация; контроль; координация.

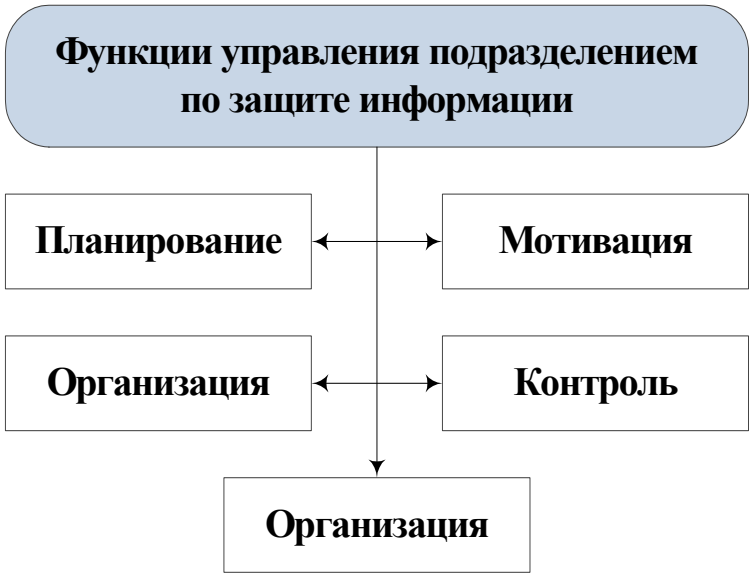

Рис. 2.1. Функции управления подразделением по защите информации

Планирование деятельности подразделения по защите информации – функция управления, связанная с определением целей управления подразделением по защите информации, поиском методов, необходимых для достижения поставленных целей на защиту информации и определением системы показателей, определяющих эффективность применения методов для достижения поставленных целей. Результатом планирования является план.

Организация деятельности подразделения по защите информации – функция управления, обеспечивающая переход подразделения по защите информации из существующего состояния в планируемое состояние. Данная функция включает распределение работы среди сотрудников подразделения по защите информации, группировку задач по защите информации в логические блоки, создание подразделений по защите информации и координация их работы.

Мотивация деятельности сотрудников подразделения по защите информации – функция управления, которая предусматривает создание у сотрудников подразделения по защите информации внутреннего побуждения к действиям для достижения поставленных целей перед подразделением по защите информации в соответствии с делегированными им обязанностями и согласно планам.

Контроль деятельности подразделения по защите информации – функция управления, предусматривающая определение показателей оценки эффективности деятельности подразделения (сотрудника) по защите информации, задание требуемых значений для них,

их измерение и сравнение полученных значений с заданными, корректировку управленческих процессов, если значения измеренных показателей существенно отличаются от их требуемых значений.

Координация деятельности подразделения по защите информации – функция управления, состоящая в согласовании и установлении функциональной взаимозависимости методов по защите информации для достижения целей защиты информации. Взаимосвязь функций управления подразделением по защите информации показана на рис. 2.2.

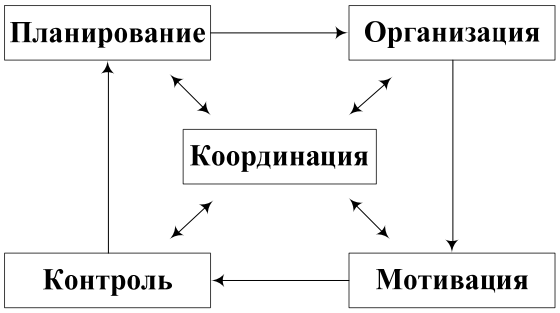

Рис. 2.2. Взаимосвязь функций управления подразделением по защите информации.

Конкретные функции управления связаны со спецификой объекта управления. Выделение конкретных функций управления необходимо для организации управления, формирования штатов и организационной структуры подразделения по защите информации.

Так как конкретные функции возникают в результате наложения функций управления на специфику объектов управления, то перечень таких функций зависит от перечня объектов управления и уровня декомпозиции самих функций.

В качестве объектов управления в области защиты информации могут выступать (рис. 2.3):

Рис. 2.3. Объекты управления в области защиты информации

- ресурсы, выделяемые на защиту информации;
- процессы защиты информации;
- результаты защиты информации.

Эта классификация представляет организацию защиты информации как совокупность входов, выходов. При этом рассматриваются процессы преобразования ресурсов на входе в результаты на выходе.

Функции управления ресурсами, выделяемыми на защиту информации. Подразделение по защите информации в процессе своей деятельности использует материальные, трудовые, финансовые, информационные, технологические и другие ресурсы. Соответственно выделяют конкретные функции управления:

управление силами защиты информации;

управление средствами защиты информации;

управление технологиями защиты информации.

Основные функции управления представлены на рисунке 2.4.

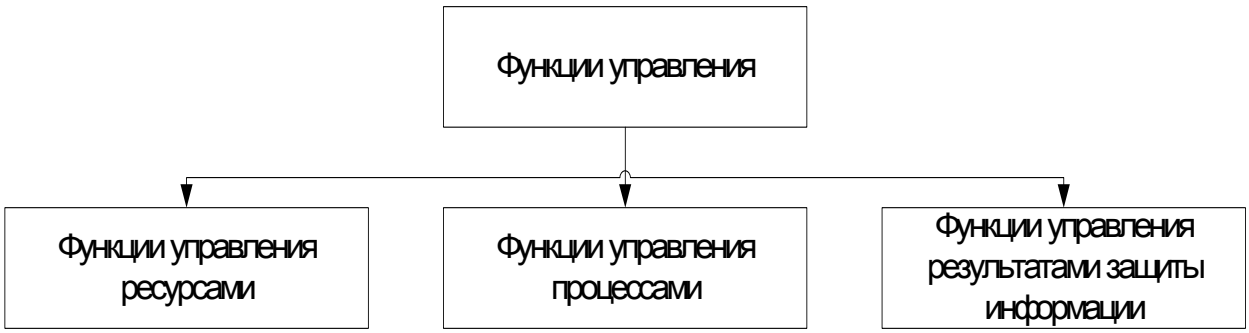

Рис. 2.4. Функции управления объектов защиты информации

Функции управления процессами защиты информации. В подразделении по защите информации протекает множество процессов, начиная от самого общего процесса управления подразделением, и до более конкретных: процессы реализации общих функций управления, процессы коммуникаций, принятия решений, производственный процесс. В соответствии с этим выделяют конкретные функции управления:
управление материально-техническим снабжением подразделения по защите информации;
управление процессом защиты информации;
управление вспомогательными процессами для обеспечения защиты информации;
совершенствование управления подразделением по защите информации.
Функции управления результатами защиты информации. К результатам (выходам системы) относят: прибыль организации, рентабельность подразделения по защите информации, затраты на защиту информации, качество работ по защите информации и т.д. Соответственно выделяют конкретные функции управления:
управление качеством работы подразделения по защите информации;
управление затратами на защиту информации и т.д.
Литература: 1,2,3,4

Тема 3 Структура и штаты службы; подбор, расстановка и обучение сотрудников службы

В рамках работы конкретного предприятия или организации можно выделить такие типовые организационные структуры:

Служба ЗИ – централизованно управляемая, совокупность структурных подразделений по ЗИ объединённая общими целями, функциями и объектами управления.

Отдел ЗИ – отраслевое и функциональное, структурное подразделение по ЗИ, осуществляющее исполнительные и организационно-распорядительные функции, отнесённые к его введенью в пределах одного из направлений деятельности по ЗИ.

Лаборатория – это структурное подразделение по ЗИ, которое осуществляет исполнительные и организационно-распорядительные функции по исследованию вопросов ЗИ, возможностей реализации, средств и технологий защиты информации.

Сектор/группа по ЗИ – это структурное подразделение отдела/отделения по ЗИ, осуществляющее исполнительную деятельность, возглавляемое главным специалистом или старшим инженером, и объединяющее 2-х или более специалистов по ЗИ, инженеров, техников в одном тематическом направлении деятельности отдела/отделения

Подразделение ЗИ – является, структурированным подразделением, официально выделенным.

Отделение ЗИ – как отдел ЗИ (может быть узконаправленное)

Наименование подразделения по ЗИ должно содержать основное функциональное направление (вид деятельности). Структура подразделения по ЗИ зависит от факторов:
- численности работников

Подходы к созданию службы ЗИ:

1) Создание полноценной службы по исполняемым функциям.

Предполагает отказ от услуг сторонних структур и передачу всех функций, полномочий и ответственности за ИБ собственной службе ЗИ (безопасности).

Преимущества: полное исполнение функции (реагирование), оперативность и эффективность.

Недостатки: большие затраты, кадровое обеспечение (ресурсы).

2) Создание службы ЗИ, минимизированной по исполняемым функциям

Привлечение сторонних организаций.

Преимущества: маленькие затраты, нет необходимости приобретать дорогую технику.

Недостатки: низкая оперативность решения, степень доверия и ответственности к сторонней организации.

3) Создание службы ЗИ с ограниченными функциями

Практическая работа: Разработка организационно-правовых аспектов деятельности службы защиты информации

Литература: 1,2,3,4

Тема 4 Организационные основы и принципы деятельности службы

Организационная структура управления подразделением по ЗИ

Организационная система – такая система, структурными элементами которой являются люди, осуществляющие преобразование ресурсов этой системы. Каждый элемент системы принимает решение на организацию определённых действий, т.е. является решающим.

Элементы, которые принимают решение по организации только собственных действий - это исполнительные элементы. Руководящие принимают решения и для других элементов.

Основной элемент – люди, сотрудники

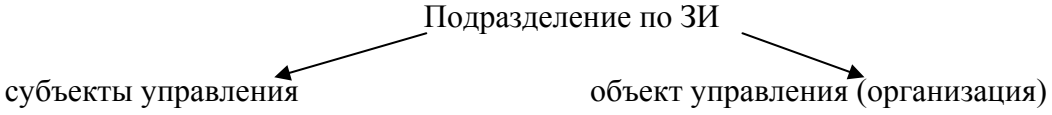

Рис. 4.1 – Объектный состав СУ СЗИ

Субъекты – они являются организаторами, работа заключается в управлении и контролем над исполнением. Объекты – исполнители, воздействующие на определённые объекты труда (непосредственное выполнение мероприятий по ЗИ);

Обеспечивающие подсистемы выполняют вспомогательное обслуживание.

Орг. структура управления – это состав и формы взаимодействия единиц и звеньев, выполняющих функцию управления подразделением по ЗИ.

ОСУ – состав (специализация), взаимосвязи, соподчинённость самостоятельных управленческих подразделений и отдельных сотрудников по ЗИ.

Сущность и содержание ОСУ подразделения по ЗИ, проявляется в её функциях, а форма - в организационных структурах.

В любой ОСУ существуют уровни и звенья управления.

Звено управления – организационно обособленное самостоятельное структурное подразделение по ЗИ или группа сотрудников по ЗИ, объединённая общим видом деятельности.

Уровни управления — совокупность звеньев управления ЗИ, находящихся на одном горизонтальном уровне и показывающая последовательность органов управления.

Создание ОСУ предприятия по ЗИ, связанно с определением составляющих, чтобы определить организационную структуру:

Составляющие ОСУ:

1. Состав и содержание функций управления ЗИ

2. Степень централизации и децентрализации функции ЗИ, а также число уровней управления
3. Число линейных и функциональных звеньев управления ЗИ каждого уровня
4. Функции каждого звена управления ЗИ всех уровней
5. Подчинённость между звеньями в управлении ЗИ всех уровней

Порядок функционирования подразделения по ЗИ, который зависит от функций, взаимодействовать с внутренней/внешней средой.

*Факторы, влияющие на построение ОСУ, три группы:*технологические, организационные, производственный фактор, организационная структура.

Рис. 4.2. Факторы влияющие на создание ОСУ

Требования, предъявляемые к ОС, подразделения по ЗИ: направленность на достижение целей ЗИ, способность к развитию, согласованность интересов, экономичность, перспективность, индивидуализация, управляемость.

1. Достигается с помощью установления правил и необходимой полноты ответственности каждого управляющего звена. Кроме того для реализации необходимо учитывать рациональное разделение и кооперацию труда между звеньями и уровнями управления.

2. Технология ЗИ постоянно совершенствуется, изменяются внешние условия. ОСУ должна быть гибкой и восприимчивой к коррекции.

3. В ОСУ должны быть заложены механизмы, которые могут (позволяют) установить противоречия, возникающие внутри и между подразделениями.

4. ОСУ должна способствовать рациональному осуществлению процессов управления.

5. ОСУ не должна решать только оперативные задачи ЗИ, а должна быть ориентирована на определённые стратегии развития организации в целом.

6. Каждое подразделение по ЗИ имеет свои особенности (кадры, оборудование, формальные, неформальные связи), следовательно, каждая ОСУ индивидуальна.

7. Требования, учитывающие допустимое число сотрудников подчинённых одному руководителю в данном подразделении по ЗИ.

Виды ОСУ подразделения по ЗИ: линейная, функциональная, линейно-функциональная, линейно-штабная, программно-целевая (матричная).

Каждая ОСУ строится по иерархическому признаку.

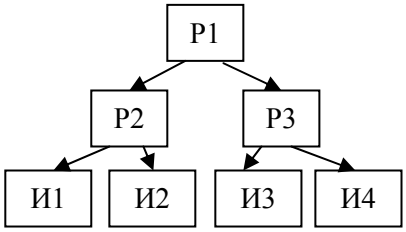

Рис. 4.3. Линейная

Во главе стоит руководитель, руководит со всеми полномочиями, единоличное руководство (сверху вниз). Решения передаются по цепочке и являются обязательными для ниже-

стоящих. Достоинства: простота, полная ответственность линейного руководителя за работу подчинённых. Недостатки: высокие требования к линейным руководителям, отсутствуют звенья по стратегическому планированию, вопросы текучки, малая гибкость, результаты работы всего зависят качества решений

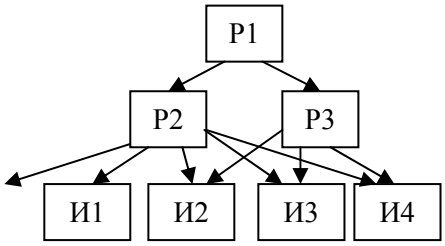

Рис.4.4. Функциональная

Каждому функциональному руководителю подчиняются все подчиненные из каждой группы. Достоинства: уровень принимаемых решений повышается за счёт специализации управления, быстродействие решения задач. Недостатки: дуализм управления, двойная подчинённость (нарушение принципа единоначалия).

Линейно-функциональная. Синтез линейной и функциональной, формируются сектора и группы. Достоинства: обоснованность команд управления, единоначалие, линейный руководитель несёт ответственность за решения. Недостатки: затруднение выработки решений, увеличение сроков принятия решений

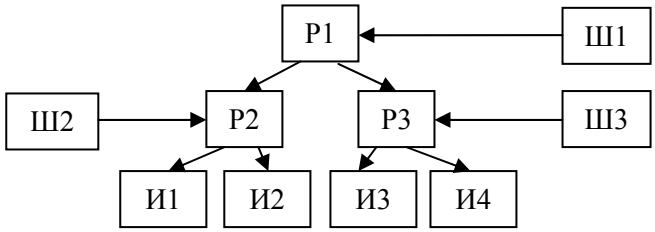

Рис.4.5. Линейно-штабная

Штаб вырабатывает решения, которые доводят линейному руководителю.
Появляются руководители проектов

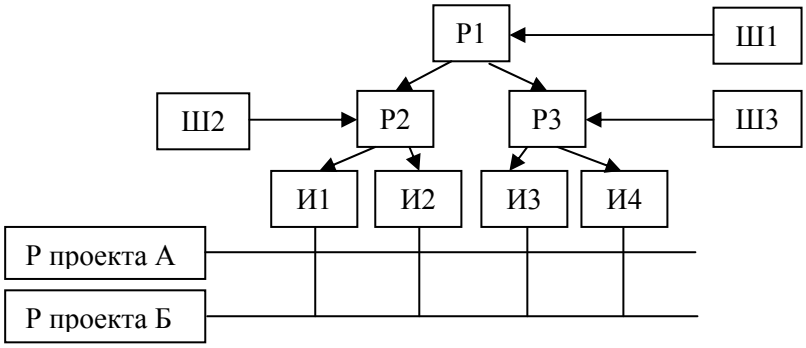

Рис. 4.6. Матричная

Организационно-штатное обеспечение службы защиты информации.
Организационно-штатная работа включает в себя:

- обобщение и анализ изменений в деятельности службы и подготовку предложений по приведению его организационно-штатной структуры в соответствие с объемом выполняемых задач;
- разработку структуры и формирование штатов службы и подчиненных ему подразделений;
- учет и анализ штатной численности службы по категориям и подразделениям;
- выработку предложений по наиболее рациональному и эффективному использованию имеющихся сил и средств, распределению и перераспределению имеющейся и дополнительно выделенной штатной численности;
- расчет нагрузки на сотрудников всех подразделений службы безопасности.

Принципы организации СЗИ

Выражает основополагающие требования, тактики по организации деятельности.

1. Законность: меры по ЗИ разрабатывается на основе норм права в пределах, определенных типовым положением.
2. Самостоятельность и ответственность: СЗИ располагает всеми необходимыми для своей деятельности видами ресурсов, при использовании которых обеспечивается строгое соответствие производимых затрат и достигнутых результатов, материальную ответственность инициаторов и исполнителей соотв-х мероприятий за результаты своей деятельности.
3. Экономическая целесообразность: мероприятия по информационной безопасности предприятия не должны приводить к ухудшению экономич. показателей, а стабильность является главным критерием оценки качества работы СЗИ.
4. Специализация и профессионализм: кадровый состав подразделения специализируется по направлению комплексного обеспечения безопасности предприятия; профессиональня подготовка сотрудников должна позволять использовать современные достижения и методы в сфере защиты информации.
5. Программно – целевое планирование; осуществляется на основании комплексной программы и разработках на её основе плановых работ и отдельных мероприятий.
6. Взаимодействия и координация: функционирование осуществляется на основе взаимодействия и скоординированости усилий всех заинтересованных подразделений, а также установление необходимых связей с внешними органами (орг. гос. упр., правоохр. орг., др. предприятия и фирмы) деятельность СЗИ не должна нарушать норм деятельности предприятия

Общая структура нормативной документации по обеспечению безопасности информации в организации

1. Документы *концептуального* уровня разрабатываются руководителями организаций с привлечением технических специалистов, юристов и т.д.

Особенности – они отражают права организации в области ЗИ и основные положения по обеспечению безопасности в организации. Являются базовыми, на их основе определяется: политика безопасности, структура органов ИБ, оцениваются риски и угрозы безопасности информации, проводится единая техническая политика.

Они носят рамочный характер (Устав организации, Концепция ИБ, модель ЗИ в организации).

2**.** Документы *общего* уровня (применения).

Особенности – документы разрабатывает служба ЗИ. Утверждает руководитель организации. Содержание требования к подразделениям и части сотрудников связанных с обработкой защищаемой информаций. Определяют общие принципы работы в штатной/нештатной ситуации.

Политика безопасности информации, положение о категорировании ресурсов в организации, положение о конфиденциальности информации и категорировании, разрабатывается порядок обращения с защищаемой информацией, положение о подразделении по ЗИ и должностные инструкции этого подразделения, инструкции о порядке действий в нештатных ситуациях.

3. Документы, регламентирующие работу персонала с защищаемыми носителями. Разрабатываются подразделением по ЗИ, согласовываются с руководителями заинтересованных подразделений, утверждаются руководителем службы ИБ.

Основное содержание направленно на установление типовых действий персонала с носителями защищаемой информации.

Инструкции по работе с ключевыми материалами, по организации антивирусной защиты, парольной защиты, инструкции по внесению изменении в списки пользователей, по резервному копированию, по модификации программных и технических средств, по работе с эталонным ПО, положение об администраторе безопасности.

Характеристика отдельных нормативных документов по обеспечению безопасности информации в организации

Характеристика отдельных нормативных документов

Устав.

В нём отражены вопросы о целях деятельности по ЗИ, обязанности сотрудников организации по вопросам соблюдения режима конфиденциальности, вопросы по деятельности организации.

Концепция информационной безопасности.

Формализует подход к обеспечению ПБ, определяет системный подход. Цель концепции – формирование интегрированной системы взглядов на цели, задачи основные принципы и направления деятельности в области ИБ согласно действующему законодательству и международным стандартам.

Это основополагающий документ, отражает ключевые положения по ЗИ, принципы и стратегические решения в области безопасности информации.

Описывает вопросы безопасности информации на всех этапах. Должна содержать:

1) Общую характеристику объекта защиты;
2) Формулировку целей создания системы защиты;
3) Основные задачи для решения поставленных целей;
4) Перечень типовых угроз безопасности информации, пути реализации этих угроз;
5) Неформальная модель нарушителя;
6) Методы и средства, которые будут применяться для решения задач;
7) Модель защиты.

Политика безопасности.

Совокупность управленческих решений, направленных на защиту информационных ресурсов. Особенность – охват всех технологических процессов связанных с информацией.

Положение о категорировании ресурсов.

Определяет объекты подлежащие защите и приоритеты при организации защиты.

1) Цель введения классификации
2) предложение по числу и названию категорий
3) определить меры и средства по ЗИ которые будут обязательны и рекомендуемые
4) образец формуляра ресурса
5) образец формуляра задач

Положение о порядке обращения с информацией подлежащей защите.

Отражает виды защищаемых ресурсов, порядок хранения, уничтожения, передачу другим лицам конфиденциальных документов, ответственность за нарушение и т.д.

Положение о подразделении ЗИ.

Общее руководство по руководству, функциям, задачам, правам, обязанностям, ответственности и штатной структуре.

Положение о ключевых носителях (материальных), где разработчик не указал (криптография).

Инструкция по работе с эталонным ПО

Инструкция о резервном копировании

Порядок восстановления данных

Процесс получения носителя

Пример: ввод в эксплуатацию канала связи - (КИБ, модель ЗИЮ ПИБ, положение о категорировании ресурсов, инструкции о порядке внешних систем);
ввод в эксплуатацию рабочих станции - (КИБ, ПИБ, категории, пароли, антивирусы, администраторы)

Положение «о подразделении по ЗИ организации»

Положение – это правовой акт, который определяет порядок образования подразделения, его права, обязанности, ответственность и организацию работ.

Заголовок отвечает на вопрос «о чём». Документ разрабатывает отдел кадров или будущий начальник подразделения (и потом согласует с отделом кадров и др. подразделениями). Существуют две модели положения. Две модели, могут отличаться по содержанию.

Первая: общие положения; структура, штатная численность; задачи; функции; права; взаимоотношение (служебные связи); ответственность.

Вторая: общие положения; цели и задачи подразделения; функции подразделения; права и обязанности подразделения; ответственность; взаимодействие подразделения; имущество и средства; трудовые отношения; организация работ; структура и штатная численность; финансирование работ и материально-техническое обеспечение подразделения.

Макет: бланк, правый верхний угол – утверждено, о чём, разделы.

Наименование организации должно соответствовать названию в учредительных документах. Гриф об утверждении – утверждается руководителем или лицом имеющим право на это. Может утверждаться в качестве приказа.

Литература: 1,2,3,4

Практическая работа: Разработка организационно-правовых аспектов деятельности службы защиты информации

Практическая работа: Разработка организационной структуры службы защиты информации

Тема 5 Организация труда сотрудников службы

Под организацией труда понимаются конкретные формы и методы соединения людей и техники в процессе труда. Организация труда всегда имеет две стороны: естественно-техническую и социально-экономическую. Эти стороны тесно связаны между собой и находятся в постоянном взаимодействии, определяя содержание организации труда.

В содержании организации труда, исходя из особенностей решаемых задач, выделяют ряд направлений (элементов). Основные из них:

Таблица 5.1

Направления организации труда

Направления	**Характеристика направлений**
разделение труда	Обоснованное распределение работников по объединенным в определенную систему трудовым функциям и рабочим местам, а также в соответствующую группировку и комбинирование работников в коллективы
нормирование труда	предполагающее тщательный расчет норм затрат труда на производство продукции и услуг как основу для организации труда и определения эффективности производства
организация и обслуживание рабочих мест	охватывающая их рациональную планировку и оснащение, эффективную систему обслуживания рабочих мест, аттестацию и рационализацию рабочих мест
организация подбора персонала и его развитие	включающие в себя: планирование персонала, профориентацию и профотбор, найм персонала, разработку концепции развития персонала и ее реализацию (квалификационный рост, планирование карьеры и др.)
улучшение условий труда	предусматривающее устранение вредности производства, тяжелых физических, психологических и эмоциональных нагрузок, внедрение эс-

	тетики в производственную среду, формирование системы охраны и безопасности труда
эффективное использование рабочего времени	оптимизация режимов труда и отдыха
рационализация трудовых процессов	внедрение оптимальных приемов и методов труда, включающие в себя изучение трудовых процессов с применением различных способов и технических средств, отбор наиболее рациональных приемов и методов труда, их совершенствование и внедрение путем организации производственного инструктажа, обучения; расширение и обновление научно-технической информаци
укрепление дисциплины труда	предусматривающее комплекс мер по усилению дисциплины, организационных мер по соблюдению конфиденциальности информации

Многообразие форм организации труда предопределяется прежде всего различием качественного расчленения и количественной пропорциональности в обеспечении информационной безопасности процессов.

Из множества других причин, вызывающих многообразие конкретных форм организации труда можно выделить ряд основных: научно-технический прогресс, систематическое совершенствование техники и технологиисистема организации предприятия или организации; психофизиологические факторы; факторы, связанные с характером задач, решаемых в разных звеньях системы информационной безопасности.

Организация труда должна рассматриваться с двух сторон: во-первых, как состояние системы, имеющей вышеназванные вполне конкретные взаимосвязанные элементы и отвечающей целям организации в целом, во-вторых, как систематическая деятельность людей по осуществлению основных процессов.

Организация труда имеет изменяющееся содержание, определяемое совершенствованием технической и технологической базы информатизации. Каждому достигнутому уровню техники и технологии соответствуют свои формы организации труда.

Управление является необходимым и очень важным звеном в системе организации труда и особой и важной трудовой функцией.

Эта трудовая функция имеет своим содержанием организацию деятельности людей и использования средств производства, при этом управление охватывает широкий круг вопросов, связанных с функционированием различных служб предприятия – технических, организационных, экономических. Все это и обусловило выделение понятия «организация управления». Вместе с тем в управлении, как и в производстве, заняты люди, труд которых должен быть соответствующим образом организован. Отсюда вытекает необходимость понятия *«организация управленческого труда», отражающего одно из направлений в организации труда в целом.*

Основные принципы организации труда. Практическое осуществления мер по организации труда в современных условиях основано на соблюдении ряда принципов:

- системного подхода к решению комплекса задач по организации труда
- планомерности, предусматривающая планирование количественного и качественного состава трудового коллектива, нормативной базы;
- научной обоснованности, заключающийся в использовании научной рекомендации по работе кадрами, всесторонние обосновании нормативной базы.

Литература: 1,2,3,4

Практическая работа: Разработка модели системы защиты информации для службы защиты информации.

Практическая работа: Оценка производительности труда по результатам оптимизации процессов в службе защиты информации

Тема 6 Принципы, методы и технология управления службой

Принципы. Поскольку информационная безопасность должна быть связующим звеном между политикой безопасности и информационной политикой, то логично было бы проводить ее по единым принципам, общим и для национальной безопасности, и для информационной политики. В Концепции национальной безопасности по ряду принципов, закрепленных в Законе РФ «О безопасности», раскрыто их содержание (приведено в скобках) [4]:

- законность (соблюдение Конституции Российской Федерации, законодательства Российской Федерации и норм международного права при осуществлении деятельности по обеспечению национальной безопасности);
- соблюдение баланса жизненно важных интересов личности, общества и государства (единство, взаимосвязь и сбалансированность всех видов безопасности, гибкое изменение их приоритетности в зависимости от ситуации);
- не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом (уважение прав и свобод человека).

Информационная политика в любой СЗИ должна опираться на следующие базовые принципы:

- открытости политики (все основные мероприятия информационной политики открыто обсуждаются обществом и государство учитывает общественное мнение);
- равенства интересов (политика в равной степени учитывает интересы всех участников информационной деятельности вне зависимости от их положения в обществе, формы собственности и государственной принадлежности);
- системности (при реализации принятых решений по изменению состояния одного из объектов регулирования должны учитываться его последствия для состояния других и всех в совокупности);
- приоритетности отечественного производителя (при равных условиях приоритет отдается конкурентоспособному отечественному производителю информационно-коммуникационных средств, продуктов и услуг);
- социальной ориентации (основные мероприятия ГИП должны быть направлены на обеспечение социальных интересов граждан России);
- государственной поддержки (мероприятия информационной политики, направленные на информационное развитие социальной сферы, финансируются преимущественно государством);
- приоритетности права (развитие и применение правовых и экономических методов имеют приоритет перед любыми формами административных решений проблем информационной сферы).

Правовое обеспечение информационной безопасности должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов в информационной сфере:

- принцип законности требует при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в данной сфере;
- принцип баланса интересов в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях и использование форм контроля деятельности.

Принципы реализации системы защиты информации.

Принципы реализации СЗИ: принцип комплексности и индивидуальности; последовательности рубежей безопасности; равнопрочности и равномощности; адекватности и эффективности: СЗ должна соответствовать возможной угрозе; секретности; адаптивности: СЗ должна быть гибкой для изменения без ущерба существования; экономичности; эффективного контроля; регистрации (найти слабое звено); защита средств обеспечения защиты.

Методы управления подразделенем по ЗИ

Методы управления подразделением по ЗИ: экономические, организационно-распорядительные, правовые, социально-психологические.

Экономические основаны на экономических законах, заключаются в стимулировании и поощрении.

Организационно-распорядительные. Дополняют экономические методы и регламентируют сроки исполнения и круг лиц, ответственных за каждый участок работы:

Бывают: 1) организационного воздействия:

– метод организационного регулирования на каждом уровне
– организационного планирования (системы нормативов для выполнения работ)
– организационные нормативы (объём работ)

2) распорядительные:

– технические нормы (регламент и стандарты)
– метод организационного инструктирования (позволяет ответственному выполнять определение функций.)
– метод распорядительного воздействия (используется при возникновении отклонений от запланированных способов выполнения работ) - приказы, распоряжения, устные указания.
– экономические нормативы

Правовые — предполагают использование различных видов ответственности за нарушения или невыполнение нормативно-правовых актов.

Социально психологические — воздействуют на систему управления через стимулы и мотивы:

– повышение мотивации на результат выполнения работ
– развитие социальных потребностей и интересов
– повышение деловой активности
– усиление ответственности работников за выполнение поставленных задач
– повышение квалификации
– предотвращение и устранение конфликтных ситуаций.

Основные классы мер процедурного уровня информационной безопасности [5]:

– Управление персоналом
– Физическая защита
– Поддержание работоспособности
– Реагирование на нарушения режима безопасности
– Планирование восстановительных работ

В рамках реализаций функций управления важно рассмотреть вопросы управления персоналом. Управление персоналом начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существуют два общих принципа, которые следует иметь в виду: разделение обязанностей; минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотребителей.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т.д. Подобная процедура может быть длительной и дорогой, по-

этому нет смысла дополнительно усложнять ее. В то же время неразумно и совсем отказываться от предварительной проверки, чтобы случайно не принять на работу человека с уголовным прошлым или психическим заболеванием.

Когда кандидат определен, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить с его служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно.

В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенно аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале – одновременно с извещением о наказании и увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

Проблема Обучения – одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политической безопасностью своей организации, он не может стремиться к достижению сформулированных в ней целей. Не зная мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

Понятие технологии обеспечения информационной безопасности [19]

Под *технологией обеспечения информационной безопасности в ИС* понимается определенное распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников (должностных лиц) организации по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.

Требования к технологии управления безопасностью:

• соответствие современному уровню развития информационных 4; технологий;

• учет особенностей построения и функционирования различных подсистем АС;

• точная и своевременная реализация политики безопасности организации;

• минимизация затрат на реализацию самой технологии обеспечения безопасности.

Для реализации технологии обеспечения безопасности в АС необходимо:

• наличие полной и непротиворечивой правовой базы (системы взаимоувязанных нормативно - методических и организационно -распорядительных документов) по вопросам ОИБ;

• распределение функций и определение порядка взаимодействия подразделений и должностных лиц организации по вопросам ОИБ на всех этапах жизненного цикла подсистем АС, обеспечивающее четкое разделение их полномочий и ответственности;

• наличие специального органа (подразделения защиты информации, обеспечения информационной безопасности), наделенного необходимыми полномочиями и непосредственно отвечающего за формирование и реализацию единой политики информационной безопасности организации и осуществляющего контроль и координацию действий всех подразделений и сотрудников организации по вопросам ОИБ.

Реализация технологии ОИБ предполагает:

• назначение и подготовку должностных лиц (сотрудников), ответственных за организацию, реализацию функций и осуществление конкретных практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

• строгий учет всех подлежащих защите ресурсов системы (информации, ее носителей, процессов обработки) и определение требований к организационно-техническим мерам и средствам их защиты;

• разработку реально выполнимых и непротиворечивых организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• реализацию (реорганизацию) технологических процессов обработки информации в АС с учетом требований по информационной безопасности;

• принятие эффективных мер сохранности и обеспечения физической целостности технических средств и поддержку необходимого уровня защищенности компонентов АС;

• применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывную административную поддержку их использования;

• регламентацию всех процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников структурных подразделений, использующих АС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• четкое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• персональную ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;

• эффективный контроль за соблюдением сотрудниками подразделений - пользователями и обслуживающим АС персоналом, - требований по обеспечению безопасности информации;

• проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработку и реализацию предложений по совершенствованию системы защиты информации в АС.

Организационные (административные) меры регламентируют процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Литература: 1,2,3,4

Практическая работа: Экспертная оценка мероприятий по защите информации в службе защиты информации

Практическая работа: Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации

3. Практические занятия

Перечень практических работ

Тема лекции	*Тема практической работы*
Тема 3 Структура и штаты службы; подбор, расстановка и обучение сотрудников службы. Тема 4 Организационные основы и принципы деятельности службы	Разработка организационно-правовых аспектов деятельности службы защиты информации
Тема 4 Организационные основы и принципы деятельности службы	Разработка организационной структуры службы защиты информации
Тема 5 Организация труда сотрудников службы	Разработка модели системы защиты информации для службы защиты информации
Тема 5 Организация труда сотрудников службы	Оценка производительности труда по результатам оптимизации процессов в службе защиты информации
Тема 6 Принципы, методы и технология управления службой	Экспертная оценка мероприятий по защите информации в службе защиты информации
Тема 6 Принципы, методы и технология управления службой	Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации

ПРАКТИЧЕСКАЯ РАБОТА № 1
Разработка организационно-правовых аспектов деятельности службы защиты информации

Цель работы: создание базы организационно-распорядительных документов

Задание: Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации

Теоретические аспекты содержания лабораторной работы

Защита информационных ресурсов реализуется в рамках нескольких направлений деятельности СЗИ. Это решение научно-технических проблем, правовое регулирование отношений в процессе информатизации деятельности любой организации.

Разработка организационно-правового обеспечение защиты информации является актуальной в связи с признанием за информацией статуса товара, продукта общественного производства, установления в законодательном порядке права собственности на информацию.Такая постановка вопроса приобретает особый смысл и характер в условиях демократизации общества, формирования рыночной экономики, включения нашего государства в мировое экономическое сообщество. Если решение вопросов развития производственной базы создания средств информатики в какой-то мере можно осуществить с использованием рыночных структур и отношений, то разработка и внедрение законодательной базы информатизации невозможны без активной государственной информационной политики, направленной на построение по единому замыслу организационно-правового механизма управления информационными процессами» увязанного с научно-технической базой информатизации.

Организационно-правовое обеспечение является многоаспектным понятием, включающим законы, решения, нормативы и правила, организационно-распорятидельные мероприятия. Применительно к защите информации, обрабатываемой в информационной системе, данный вид обеспечения имеет ряд принципиальных специфических особенностей, обусловленных следующими факторами, которые показаны на рисунке 1.1.

Рис. 1.1. Факторы, влияющие на формирование организационно-правового обеспечения защиты информации

Исходя из приведенных обстоятельств, комплекс вопросов, решаемых организационно-правовым обеспечением, может быть сгруппирован в три класса:

- организационно-правовая основа защиты информации в информационных системах;
- технико-математические аспекты организационно-правового обеспечения;
- юридические аспекты организационно-правового обеспечения защиты.

Организационно-правовая основа защиты информации должна включать (таблица 1.1).

Таблица 1.1

Структура организационно-правовой основы защиты информации

№ п/п	**Формирующие составляющие организационно-правовой основы защиты информации в службе защиты информации**
1	Определение подразделений и лиц, ответственных за организацию защиты информации
2	Нормативно-правовые, руководящие и методические материалы (документы) по защите информации
3	Меры ответственности за нарушение правил защиты
4	Порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации

Под технико-математическими аспектами организационно-правового обеспечения понимается совокупность технических средств, математических методов, моделей, алгоритмов и программ, с помощью которых в ИС могут быть соблюдены все условия, необходимые для юридического разграничения прав и ответственности относительно регламентов обращения с защищаемой информацией. Основными из этих условий являются следующие:

- фиксация на документе персональных идентификаторов ("подписей") лиц, изготовивших документ и (или) несущих ответственность за него;
- фиксация (при любой необходимости) на документе персональных идентификаторов (подписей) лиц, ознакомившихся с содержанием соответствующей информации;

- невозможность незаметного (без оставления следов) изменения содержания информации даже липами, имеющими санкции на доступ к ней,
- т.е. фиксация фактов любого (как санкционированного, так и несанкционированного) изменения информации;
- фиксация факта любого (как несанкционированного, так и санкционированного) копирования защищаемой информации.

Под юридическими аспектами организационно-правового обеспечения защиты информации в ИС понимается совокупность законов и других нормативно-правовых актов, с помощью которых достигаются следующие цели;

- устанавливается обязательность соблюдения всеми лицами, имеющими отношение к информационной системе всех правил защиты информации;
- узакониваются меры ответственности за нарушение правил защиты;
- узакониваются технико-математические решения вопросов организационно-правового обеспечения защиты информации;
- узакониваются процессуальные процедуры разрешения ситуаций. складывающихся в процесс: функционирования систем защиты.

Таким образом, вся совокупность вопросов, возникающих при решении проблем организационно-правового обеспечения, может быть представлена в виде схемы, приведенной на рис.1.2.

Рис. 1.2. Структура Организационно-правового обеспечения защиты информации, формируемого в службе защиты информации

Основополагающим понятием в области правового аспекта защиты информации является “информация”. Закон РФ “Об информации, информатизации и защите информации” определяет понятие информация как “сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления”.

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права, что дает возможность применять к информации нормы Уголовного и Гражданского права в полном объеме.

Анализ организационно-правового обеспечения планируемых к осуществлению мероприятий в области организации защиты информации всегда должен предшествовать принятию окончательного решения о реализации этих мероприятий.

К организационно-правовым мероприятиям по защите конфиденциальной информации относятся мероприятия по разработке и принятию определенных документов предприятий и организаций, регламентирующих степень и порядок допуска собственных сотрудников, а также сторонних лиц и организаций к конкретным информационным ресурсам.

Организационно-правовая защита информации реализуется путем установления на предприятии режима конфиденциальности.

Можно выделить три формы конфиденциальных отношений, что представлено в таблице 1.2.

Таблица 1.2

Формы конфиденциальных отношений

Субъекты отношений	**Реализация отношений**
Между сотрудником предприятия и самим предприятием как юридическим лицом	Реализуется на практике путем составления соответствующего трудового договора или контракта, заключаемого с сотрудником предприятия
Складывающиеся между конкретным сотрудником и другими сотрудниками этого предприятия	Эти отношения развиваются как по вертикали, так и по горизонтали. Указанные отношения называются конфиденциальными отношениями по служебным функциям. Юридически эти отношения закрепляются многообразными административно-правовыми решениями, например приказами о выполнении определенных работ, и регламентируются “Должностными инструкциями”
Складывающиеся в рамках хоздоговорных работ и базирующиеся на договоре между партнерами	Юридически конфиденциальные отношения закрепляется в виде четко сформулированных требований и обязательств, которые выдвигают договаривающиеся стороны, и фиксируют в договоре

В вопросах реализации технических мероприятий обеспечения информационной безопасности с точки зрения правового обеспечения основное внимание следует уделять выполнению требований лицензирования исполнителей работ и использования сертифицированных средств защиты, а также действующим ограничениям на применение специальных технических средств.

В существующей практике можно выделить следующие основные аспекты решения проблемы защиты информации:

- анализ правового обеспечения;
- реализация организационно-правовых мероприятий защиты;
- реализация технических мероприятий по защите информации.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом культуры работающего в этой области специалиста.

Ход работы:

1. В соответствии с предложенным вариантом организации или предприятия проанализировать организационно-правовое обеспечение защиты информации в системе деятельности предприятия в целом.

2. Выявить существующие проблемные моменты и узкие места.

3. В соответствие с Законом "Об информации, информатизации и защите информации", Законом Российской Федерации "О безопасности" описать основные подходы к разработке организационно-правового обеспечения службы защиты информации на выбранном предприятии.

4. Определить круг задач службы зашиты информации (СЗИ).

5. Сформулировать основные функции СЗИ.

6. Выделить в организационно-штатной структуре штатные единицы, обеспечиыающие реализацию данных функции и особенности взаимодействия между собой.

7. Проанализировать нормативное обеспечение деятельности СЗИ, выявить проблемы.

8.Сформировать общую структуру нормативной документации по обеспечению безопасности информации в организации в следующей иерархии:

- Документы *концептуального* уровня, которые должны быть разработаны руководителями организаций;
- Документы *общего* уровня (применения);
- Документы, регламентирующие работу персонала с защищаемыми носителями.

9. Разработать отсутствующие документы, опираясь на законодательную базу, указанную в списке литературы, а также, используя Гарант, Консультант-Плюс. Доработать несоответствующие требованиям законодательства документы.

Разработать:

1) Положение о подразделении по защите информации. Общее руководство по руководству, функциям, задачам, правам, обязанностям, ответственности и штатной структуре.

2) Положение о категорировании ресурсов.

Вопросы для самоконтроля

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

Литература: 1,2,3,4

ПРАКТИЧЕСКАЯ РАБОТА №2

Разработка организационной структуры службы защиты информации

Цель работы: Разработать организационную структуру службы защиты информации конктерной организации или предприятия

Задание: Ознакомиться с принципами системного подхода при создании оргазационной структуры

Теоретические аспекты содержания лабораторной работы

Конечной *целью создания системы обеспечения безопасности информационных технологий* является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) ИС соответствующими множеству значимых угроз методами и средствами. [19]

Обеспечение информационной безопасности - это непрерывный процесс, основное содержание которого составляет управление, - управление людьми, рисками, ресурсами, средствами защиты и т.п. Люди - обслуживающий персонал и конечные пользователи ИС, - являются неотъемлемой частью информационной (то есть *«человеко-машинной»)* системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

За формирование системы защиты и реализацию единой политики информационной безопасности организации и осуществление контроля и координации действий всех подразделений и сотрудников организации по вопросам ОИБ отвечает специальное подразделение (служба) защиты информации (обеспечения информационной безопасности).

Эффективное использование штатных (для ОС и СУБД) и дополнительных средств защиты обеспечивается системными администраторами и администраторами средств защиты. Системные администраторы обычно входят в штат подразделений автоматизации (информатизации). Администраторы дополнительных средств защиты, как правило, являются сотрудниками подразделения защиты информации.

Таким образом, организационную структуру системы обеспечения информационной безопасности ИС организации можно представить в виде, совокупности следующих уровней:

- уровень 1 - Руководство организации
- уровень 2 - Подразделение организующее защиту информации и реализующее политику безопасности
- уровень 3 - Администраторы штатных и дополнительных средств защиты
- уровень 4 - Ответственные за организацию информационной безопасности в подразделениях (на технологических участках)
- уровень 5 - Конечные пользователи и обслуживающий персонал

Совокупность действий по разработке рациональной структуры и организационной поддержке службы информационной безопасности:

1. Определение задач и выделение фцнкций СЗИ.
2. Организация административной поддержки СЗИ.
3. Определение состава СЗИ.
4. Определение организационно-правового статуса СЗИ и разработка организационной структуры.

Разработка рациональной структуры службы ЗИ на предприятии, достаточной по составу и оснащению средствами управления безопасностью, возможно на основе тщательного анализа избранной политики безопасности, соотнесения вероятных угроз и потерь в случае их реализации с эффективностью системы защиты информации и финансовыми затратами на их реализацию. Это позволит обоснованно принять решение на создание соответствующей службы информационной безопасности.

Организационно-правовой статус СЗИ определяется следующим образом:

– численность службы должна быть достаточной для выполнения всех перечисленных выше функций;

– служба должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;

– штатный состав службы не должен иметь других обязанностей, связанных с функционированием ИС;

– сотрудники службы должны иметь право доступа во все помещения, где установлена аппаратура ИС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;

– руководителю службы должно быть предоставлено право запрещать включение в число действующих новые элементы ИС, если они не отвечают требованиям защиты информации;

– службе защиты информационной должны быть обеспечены все условия, необходимые для выполнения своих функций.

Можно выделить для систем управления персоналом три классических вида структурных связей, которые адаптируют к задачам СЗИ:

1) линейная (административное подчинение);

2) функциональная (методическое обеспечение, консультирование смежного подразделения);

3) линейно-функциональная (привлечение более компетентных руководителей, персональная ответственность исполнителей).

Состав и размер СЗИ *зависят от конкретного предприятия и задач*, которые ставятся перед ней.

Существует несколько вариантов штатного расписания такой службы. Один из них может быть таким:

– заместитель директора по безопасности и защите информации;
– администратор безопасности ИС - штатный сотрудник отдела защиты информации;
– администратор системы - штатный сотрудник отдела автоматизации;
– администраторы групп - штатные сотрудники подразделений, эксплуатирующих ИС;
– менеджеры безопасности;
– операторы

Данная структура используется в большинстве организаций, серьезно заботящихся о безопасности информации. Надежность такой структуры СЗИ обусловлена тем, что защитой информации занимается подразделение специалистов, несущих непосредственную ответственность за свою работу.

Ход работы:

Задание по лабораторной работе:

В соответствие с вариантом предметной области, предложенной преподавателем для конкретной организации или предприятия, студент разрабатывает организационную систему управления службой защиты информации в рамках общей структуры организации.

Рекомендуется максимально внимательно подойти к выбору варианта задания, учесть возможность привлечения данных и знаний специалистов, работающих в организации, которая подвергается системному анализу.

Варианты заданий для выполнения практических работ (предметные области) представлены в таблице 2.1

Таблица 2.1

№ п/п	**Наименование предметной области для выполнения задания по лабораторной работе**
1	Разработка организационной структуры СЗИ предприятия (по отраслям).
2	Разработка организационной структуры СЗИ крупной банковской системы.
3	Разработка организационной структуры СЗИ финансовых структур (инвестиционного фонда, кредитных организаций и т.д.).
4	Разработка организационной структуры СЗИ венчурного фонда.

5	Разработка организационной структуры СЗИ налоговой инспекции
6	Разработка организационной структуры СЗИ учебного заведения (ВПО, СПО)
7	Разработка организационной структуры СЗИ фирмы по продаже и обслуживанию ПК.
8	Разработка организационной структуры СЗИ предприятия муниципальных органов власти.

***Порядок выполнения работы*:**

Используя возможности MS Visio, создать графическую модель организационной структуры в соответствии с предложенным вариантом, на основе определения основных задач и функций СЗИ. Выявить проблемные моменты в структуре, предложить варианты устранения данных проблем. Разработать модель в соответствии с предложенными изменениями. Представить подробное описание структуры и особенносей взаимодействия структурных единиц, а также нормативно- регламентирующей документации.

Вопросы для самоконтроля

1. Какие типовые организационные структуры могут быть использованы при создании службы защиты информации?
2. В чем достоинства и недостатки организационных структур?
3. В соответствии, с какими принципами формируются структура и штаты службы защиты информации?
4. Каким образом определяется организационно-правовой статус службы защиты информации?

Литература: 1,2,3,4

ПРАКТИЧЕСКАЯ РАБОТА №3

Разработка модели системы защиты информации для службы защиты информации

Цель работы: Научиться проводить разработку модели системы защиты информации для службы защиты информации на основе модели политики безопасности.

Задание: Разработать модель системы защитыинформации на основе модели политики безопасности для конкретной организации.

Теоретические аспекты содержания лабораторной работы

Важной концепцией в проектировании и анализе систем информационной безопасности является модель безопасности, поскольку она включает в себя политику безопасности, которая должна быть реализована в системе. Модель – это символическое представление политики. Она преобразует желания создателей политики в набор правил, которым должна следовать компьютерная система.

Существуют различные подходы к определнию понятия «политика безопасности».[5] Так согласнос ГОСТ Р ИСО/МЭК 15408-1÷3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», более известному как «Общие критерии», политика безопасности – это одно или несколько правил и процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Под политикой безопасности понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы. Это формальная спецификация правил и рекомендаций, на основе которых пользователи используют, накапливают и распоряжаются информационными ресурсами, выражается в виде модели политики безопасности. Модель политики безопасности (TOE security policy model): структурированное представление политики безопасности, которая должна быть осуществлена в организации.

Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений. На практике это означает, что только соответствующим образом уполномоченные пользователи получат доступ к информации, и смогут осуществлять с ней только санкционированные действия.

Кроме того, формальные модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем (производители, потребители, эксперты-квалификаторы).

Использование модели безопасности защищенных информационных систем используются в следующих случаях:

– при составлении формальной спецификации политики безопасности разрабатываемой системы;

– при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;

– в процессе анализа безопасности системы в качестве эталонной модели;

– при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Политика безопасности разрабатывается для конкретной организации и зависит от реализации системы безопасности.

Разработка и реализация политики безопансоти осуществляется поэтапно:

1. Информационные ресурсы структурируются, проводится анализ рисков.

2. Определяются правила для любого процесса пользования данным видом доступа к элементам данных имеющим данную оценку ценностей.

Формальное выражение политики безопасности – модель политики безопасности.

Основная цель формулирования политики безопасности_ — определение условий, которым должно подчиняться поведение системы, проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Модели политики безопасности основаны на следующих принципах:

Система является совокупностью взаимодействующих сущностей субъектов и объектов. Система считается безопасной, если субъекты не имеют возможности нарушить принципы политики безопасности.

Все виды взаимодействия в системе моделируется установлением отношений определённого типа между субъектами и объектами. Все операции контролируются монитором взаимодействий и разрешаются или запрещаются в соответствии с политикой безопасности.

Политика безопасности задаётся в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами.

Совокупность множеств субъектов, объектов и отношений между ними, определяющее состояние системы, которое может быть безопасным или небезопасным в соответствии с критериями, предложенными в данной модели.

Модели политики безопасности. Модель Харрисона-Руззо-Ульмана

Данная модель реализует дискреционное (произвольное) управление доступом субъектов к объектам и контроль за распространением прав доступа. Предполагается, что:

S – множество субъектов (осуществляют доступ к информации)

O – множество объектов, содержащих защищаемую информацию

$R=\{r_1,\dots,r_n\}$ - конечное множество прав доступа, означающих полномочия на выполнение соответствующих действий (чтение, запись, выполнение)

Принято считать, что $S \subset O$, т.е. субъекты одновременно являются и объектами (это сделано для того, чтобы включить в область действия модели отношения между субъектами).

Поведение системы моделируется с помощью понятия состояния.

$O \times S \times R$ - пространство состояний системы

M – матрица прав доступа, описывающая текущие права доступа субъектов к объектам (строки – субъекты, столбцы – объекты)

$Q=(S,O,M)$ - текущее состояние системы

Любая ячейка матрицы $M[s,o]$ содержит набор прав доступа s к объекту o, принадлежащих множеству прав доступа R.

Ход работы:

Используя информационные системы Гарант, КонультантПлюс, руководствуясь стандартом (ГОСТ Р ИСО МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий), результатами предыдущих лабораторных работ сформировать модель организационной политики безопасности для варианта предметной области из лаб. работы №2.

Разработка модели организационной политики безопасности предшествует разработке инженерно-технических решений по системе информационной безопасности объекта, организационная политика безопасности должна представлять описание порядка предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Эффективность системы информационной безопасности объекта определяется на основе надежно поддерживаемого выполнения правил политики безопасности.

В отчете по лабораторной работе представить описание построения организационной политики безопасности в рамках следующих этапов:

· внесение в описание объекта автоматизации структуры ценности и проведение анализа риска;

· определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа.

Вопросы для самоконтроля

1. Какие отличия существуют в определении политики информационной безопасности?
2. В чем состоит отличие нормативно-методических документов политики безопасности от нормативных документов процедурного уровня?
3. Какие существуют особенности документального оформления политики безопасности?
4. Какова методология деятельности по обеспечению безопасности объекта на основе политики безопаснсоти?
5. Что представляет собой модель информационной безопасности в соответствии со стандартом: международным ISO/IEC 15408 "Информационная технология - методы защиты - критерии оценки информационной безопасности", стандартом ISO/IEC 17799 "Управление информационной безопасностью"?

Литература: 1,2,3,4

ПРАКТИЧЕСКАЯ РАБОТА №4

Оценка производительности труда по результатам оптимизации процессов в службе защиты информации

Цель работы: Научиться добавлять новых менеджеров по работе с клиентами и закреплять за ними клиентов. Научиться планировать и анализировать работу менеджеров.

Задание: Провести оценку производительности труда персонала службы защиты информации в соответствие с предложенной методикой.

Теоретические аспекты содержания лабораторной работы

Производительность труда — это экономическая категория, выражающая степень плодотворности целесообразной деятельности людей по производству материальных и духовных благ. Производительность труда определяется объемом работ, произведенных работником в единицу времени (час, смену, квартал, год) или количеством времени, затраченным на выполнение определенной работы.

Производительность труда исчисляется через систему показателей выработки и трудоемкости. Выработка рассчитывается как частное от деления объема выполненных работ на численность работников (затраты труда). Трудоемкость — делением затрат труда (численности работников) на объем работ. Показатели выработки и трудоемкости могут исчисляться в стоимостном выражении, в нормо-часах, в натуральном выражении и в условно-натуральном. Выработка характеризует объем работ (продукции) на единицу численности, а трудоемкость — затраты труда на единицу продукции (работы).

Производительность труда изменяется под воздействием факторов, которые могут быть внешними по отношению к предприятию и внутренними.

К внешним факторам относятся:

- природные — в сложных природных условиях (туман, жара, холод, влажность) производительность труда снижается;
- политические — по воле государства происходит накопление капитала в руках немногих, что приводит к массовому охлаждению к труду;
- общеэкономические — кредитная, налоговая политика, системы разрешений (лицензий) и квот, свобода предпринимательства и т. д.

Внутренние факторы:

- изменение объема и структуры производства;
- применение инновационных технологий в рамках информационных технологий;
- совершенствование организации и управления в организации;
- совершенствование организации и стимулирования труда.

Проведение анализа производительность труда осуществляется с учетом характеристики эффективности производительной деятельности в течение определенного времени.

Уровень производительности может быть измерен с помощью показателей выработки и трудоемкости.

Выработка $W = \frac{Q}{T}$

Q— объем выполненных работ при реализации процессов

T— затраты рабочего времени

Обратным показателем является трудоемкость (t)

$t = \frac{T}{Q}$

Выработка может считаться для разных периодов.

Поэтому выработка может быть вычислена как:

- Средняя часовая выработка. Это отношение объема выполненных работ к числу человеко-часов, отработанных в течение данного периода времени.

– Средняя дневная выработка**.** Показывает, какой объем работ был произведен каждый день в течение определенного периода времени. Для того чтобы вычислить среднюю дневную выработку времени, необходимо объем произведенной продукции разделить на число человеко-дней затраченных на производство данного объема (время изготовления данного объема).

– Средняя месячная выработка**.** Представляет собой отношение объема произведенных за месяц работ к среднесписочной численности рабочих. Аналогично может быть вычислена выработка за квартал или год.

$$\text{Средняя часовая выработка} = \frac{\text{Объем произведенной продукции}}{\text{Число человеко} - \text{часов, отработанных в течение данного периода времени}}$$

$$\text{Средняя дневная выработка} = \frac{\text{Объем произведенной продукции}}{\text{Число человеко} - \text{дней, отработанных всеми рабочими предприятия}}$$

$$\text{Средняя месячная выработка} = \frac{\text{Объем произведенной продукции}}{\text{Среднесписочное число рабочих (промышленно} - \text{производ. персонала)}}$$

Трудоемкость – это затраты рабочего времени на производство единицы выполняемых работ. Преимущество показателя трудоемкости в том, что он позволяет судить об эффективности затрат живого труда на разных стадиях выполнения работ на отдельном рабочем месте, т.е. проникнуть в глубину выполнения того или иного вида работ, чего нельзя сделать с помощью показателя выработки, исчисленного в стоимостном выражении.

В зависимости от состава включаемых в нее трудовых затрат различают технологическую трудоемкость, трудоемкость обслуживания, производственную трудоемкость и трудоемкость управления.

Для расчета производительности труда сотрудников службы защиты информации, необходимо пересмотреть и оптимизировать существующие процессы обеспечения информационной безопасности.

Оптимизация процессов обеспечения информационной безопасности должна учесть требования и особенности бизнес-процессов, существующие процедуры обеспечения информационной безопасности и пожелания сотрудников компании.

При оптимизации процессов обеспечения информационной безопасности должны сохраняться успешно работающие процедуры обеспечения информационной безопасности и максимально использоваться существующие средства защиты информации.

Проект оптимизации процессов обеспечения информационной безопасности включает:

– обследование компании с целью получения необходимой информации об особенностях бизнес-процессов, ожиданиях сотрудников и руководства;

– анализ существующих процессов обеспечения информационной безопасности;

– выработка предложений по оптимизации процессов обеспечения информационной безопасности;

– разработка необходимых организационно-распорядительных документов;

– доработка существующих средств защиты информации и внедрение новых.

В результате проекта по оптимизации компания получит эффективную и оправданную систему обеспечения информационной безопасности.

При оптимизации последовательно выявляются все значимые недостатки по заданному набору параметров, потом они сравниваются с критериями оптимальности и в завершение готовятся решения по устранению. По каким параметрам надо оценивать оптимальность процесса:

– качество конечного результата процесса;

– качество и содержание промежуточных результатов (по каждой процедуре);

- содержательность действий исполнителей при выполнении процедуры;
- компактность и согласованность схемы процесса;
- эффективность управления процесса.

Ход работы:

1. Для выбранного в предыдущих лабораторных работах варианта предметной области провести ИТ-консалтинговый анализ защищаемых информационных процессов.
2. Разработать модель информационных процессов на основе CASE-технологий.
3. Провести анализ существующих процессов обеспечения информационной безопасности. Выявить проблемные моменты. Выделить критерии оценки реализации данных процессов.
4. Выделить штатные единицы сотрудников, обслуживающих данные процессы. Определить выполняемые работы.
5. Изучить алгоритм оценки времени, необходимого для выполнения работ в системе защиты информации каждым из сотрудников службы защиты информации.
6. Выработать предложения по оптимизации процессов обеспечения информационной безопасности.
7. Првести расчет производительности труда сотрудников СЗИ до оптимизации процессов и после.

Вопросы для самоконтроля

1. Какие критерии оценки процессов в системе защиты информации существуют?
2. Как осущетсвляется расчет производительности труда сотрудников СЗИ?
3. По каким параметрам надо оценивать оптимальность процесса?
4. Какие из CASE-технологий можно применить для создания моделей информационных процессов в СЗИ?

Литература: 1,2,3,4

ПРАКТИЧЕСКАЯ РАБОТА №5

Экспертная оценка мероприятий по защите информации в службе защиты информации

Цель работы: Научиться проводить экспертную оценку мероприятий по защите информации в службе защиты информации

Задание: Отразить в АИС следующее:

Теоретические аспекты содержания лабораторной работы

Методы экспертных оценок – это достаточно эффективные методы в рамках системы защиты информации для оценки качества Комплексной системы обеспечения информационной безопасности.

Одним из наиболее часто применяемых подходов при экспертном определении коэффициентов весомостей – это подход предпочтения в виду своей простоты, когда каждому показателю присваивается место (ранг) в ряду показателей. При его использовании эксперта просят ранжировать все показатели в порядке их предпочтения.

При этом согласованность мнений экспертов проверяется коэффициентом конкордации Кендалла:

$$\bar{W} = \frac{\bar{12} \cdot \bar{S}}{m^2(n^3 - n)},$$

(1)

где S – сумма квадратов отклонений всех оценок рангов каждого объекта экспертизы от среднего арифметического суммы рангов; m – число экспертов; n – число ранжируемых показателей.

При этом вероятность случайного совпадения ранжировок экспертов оценивается по критерию χ^2 – Пирсона [2]. Для этого случая найдется как [2]: χ^2

$$\chi^2 = m(n-1)W, \tag{2}$$

при числе степеней свободы $\nu = n-1$.

Весовой коэффициент i-го показателя определяется по результату ранжировок n экспертов:

$$d_i = \frac{m(n+1) - \sum_{j=1}^{m} w_{ij})}{\sum_{i=1}^{n}\sum_{j=1}^{m} w_{ij}}. \tag{3}$$

Метод опроса. В опросном листе, где перечислены все ПК данного вида продукции, эксперты на основе собственного опыта должны выбрать основные ПК.

Результаты опроса подлежат статистической обработке в соответствии с решающим правилом. За решающее правило может быть выбрано единогласие экспертов или максимальное число голосов экспертов (например, более 80%), при котором ПК считается значимым, т.е. подлежащим нормированию.

Метод экспертных структурных опросников для оценки качества Комплексной системы обеспечения информационной безопасности представляет следующее: создается анкета специального вида или опросник, информация в котором необходима для проектирования защиты информации.

По составу различают три вида опросников:

1. Выбор экспертом жестко формализованных ответов (да, нет, не знаю);
2. Выбор ответа с указанием непосредственных действий или альтернативных вариантов;
3. Рекомендации эксперта по направлению защиты.

Эксперты должны быть из разных областей. При учете оценки каждого эксперта в составлении итоговой оценки учитывается стаж работы эксперта (например, стаж 30 лет – 10 баллов, 15 лет – 5 баллов), ответы данного эксперта оценивают с коэффициентом 1 только в том разделе, экспертом в котором он является, в других разделах коэффициент ниже.

Иерархическая структура комплексных показателей качества Комплексной системы обеспечения информационной безопасности разрабатывается индивидуально для конкретной организации. Пример структуры показателей представлен далее.

Детализация комплексных показателей зависит от структуры службы защиты информации, политики безопасности, организационно-правовых аспектов деятельности, инженерно-технических аспектов оцениваемого элемента конфигурации и задач оценки.

Вариант детализации в методике оценочных элементов по показателям качества: Показатель – Функциональные возможности (Functionality), критерии – Защищенность (Security), Способность к взаимодействию (Interoperability).

Вариант оценки значимости коэффициентов для каждого критерия и конкретного показателя выбирается индивидуально.

Типовая структура показателей качества:

1. Функциональные возможности (Functionality)
2. Надежность (Reliability)
3. Практичность (Usability)
4. Эффективность (Efficiency)
5. Мобильность (Portability)
6. Сопровождаемость (Maintainability)

Ход работы:

На основе Метода экспертных оценок, в зависимости от структуры службы защиты информации, политики безопасности, организационно-правовых аспектов деятельности, инженерно-технических аспектов оцениваемого элемента конфигурации и задач оценки, разработать дерево показателей и критериев оценки качества Комплексной системы обеспечения информационной безопасности. Представить пояснение к каждому показателю в виде таблицы.

Првести экспертную оценку службы защиты информации по показателям и критериям.

Вопросы для самоконтроля

1. В каких ситуациях эффективно использование экспертной квалиметрии применительно к системам информационной безопасности?
2. Какие методы экспертной оценки существуют?
3. Возникновение каких ошибок возможно при проведении экспертного оценивания?
4. Виды квалиметрических оценок.
5. Как формируется дерево показателей и критериев, какие факторы влияют на реализацию данной процедуры?

Литература: 1,2,3,4

ПРАКТИЧЕСКАЯ РАБОТА №6

Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации

***Цель работы**:* Ознакомление с организацией и проведением мониторинга безопасности информации в организации.

Задачи: разработать мероприятия по мониторингу работы службы защиты информации.

Теоретические аспекты содержания лабораторной работы

Существует ряд определений понятия «мониторинг»:

1. Мониторинг (предупредительный) – система регулярного измерения изменений, происходящих в системе или отдельных элементах, при условии регулярного применения одних и тех же принципов выборки и одного и того же инструментария для сбора данных.
2. Систематический мониторинг – постоянный, систематический сбор информации в целях наблюдения и контроля за ходом функционирования какого-либо параметра системы или элемента, прогнозирования дальнейшего поведения.

Мониторинг может включать в себя все указанные методы исследования в различных комбинациях.

Мониторинг/проверка/наблюдение – активный и интерактивный процесс в системе информационой безопасности, направленный на корректировку функционирования основных элементов.

Главная цель мониторинга – улучшение функционирования системы информационной безопасности в организации.

Задачи мониторинга:

1. Активный, плановый сбор и обработка по возможности исчерпывающих данных о состоянии системы в конкретной области для анализа ситуации.
2. Сравнение действительного состояния организационно-правовых аспектов с формально принятыми в рамках существующего законодательства.
3. Определение причин нарушений и поиск разумных решений изменения ситуации.
4. Накопление материалов, необходимых для дальнейшей деятельности в выбранном направлении.

Ключевые принципы мониторинга:

1. Детальность и точность собираемой информации, ее проверка и отчетность.

2. Конфиденциальность информации и источников.

3. Объективность.

4. Внимание по отношению к физической и социальной безопасности пострадавших, свидетелей и других источников.

Функции мониторинга:

1) Познавательная функция – диагноз ситуации (диагностический мониторинг) – проводится в тех случаях, когда точно неизвестно, какие нарушения преобладают, степень их нарушения.

2) Функция поддержки действий – сбор аргументов для того, чтобы убедить административный персонал в необходимости изменений.

Профилактическая функция или наблюдение, контроль.

В рамках проведения мероприятий по мониторингу возможно также организация «аудита информационной безопасности».

Данное понятие появилось сравнительно недавно. Однако, на сегодняшний день нет устоявшегося определения аудита ИБ. Его основная задача – объективно оценить текущее состояние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином «аудит информационной безопасности корпоративной системы» обычно понимается *системный процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности компании в соответствии с определенными критериями и показателями безопасности.* Считается, что результаты качественно выполненного аудита ИБ компании позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную ее текущим задачам и целям бизнеса.

Таким образом, формально аудит ИБ в информационной системе — это процесс сбора сведений, позволяющих установить:

- обеспечивается ли безопасность ресурсов организации (включая данные);
- обеспечиваются ли необходимые параметры целостности и доступности данных;
- достигаются ли цели организации в части эффективности информационных технологий.

Аудит ИБ представляет собой комплекс работ по исследованию всех аспектов обеспечения ИБ в организации, проводимых по согласованному с Заказчиком плану в соответствии с выбранной методикой и критериями. Основными целями при этом являются:

- независимая оценка текущего состояния;
- идентификация и ликвидация уязвимостей;
- технико-экономическое обоснование механизмов безопасности;
- обеспечение соответствия требованиям действующего законодательства;
- минимизация ущерба от инцидентов, связанных с нарушением информационной безопасности.

Основным продуктом аудита является аудиторский отчет, который содержит описание текущего состояния информационной безопасности в организации, описание обнаруженных уязвимостей и рекомендации по их устранению.

Ход работы:

В соответствии с выбранным вариантом предметной области для конкретной организации разработать мероприятия по мониторингу и аудиту информационной безопасности в службе защиты информации. Описать процедуры мониторинга и аудита поэтапно.

Проведение мониторинга и аудита ИБ складывается из следующих основных этапов:

1) инициирование процедуры мониторинга и аудита;
2) сбор исходных данных;
3) анализ данных мониторинга и аудита;
4) использование методов анализа рисков (необязательно);
5) оценка соответствия требованиям стандартов (необязательно);
6) выработка рекомендаций;

7) подготовка отчетной документации.

Оформить отчетные материалы по аудиту с учетом ответов на следующие вопросы:

1) Соответствует ли корпоративная система ИБ целям и задачам бизнеса компании?

2) Насколько адекватна принятая политика безопасности задачам компании и целям бизнеса?

3) Как корректно контролировать реализацию и выполнение политики безопасности в компании?

4) Когда необходимо провести модернизацию системы защиты информации и как обосновать необходимость модернизации и затрат на неё?

5) Как быстро окупятся инвестиции в корпоративную систему защиты информации?

6) Насколько правильно и корректно сконфигурированы и настроены штатные средства обеспечения защиты информации в компании?

7) Эффективно ли справляются со своими задачами существующие в компании средства защиты: межсетевые экраны (firewalls), системы обнаружения вторжений (IDS), система антивирусной защиты, VPN-шлюзы?

8) Как решаются вопросы обеспечения конфиденциальности, доступности и целостности информации при реализации бизнес-процессов?

9) Как обеспечить необходимую в деятельности организации «вертикаль власти» для осуществления централизованного управления безопасностью компании?

10) Как контролировать состояние информационной безопасности компании и какие методы и средства необходимо использовать для осуществления контроля?

11) Существуют ли стратегический и тактические планы развития системы защиты информации в компании?

12) Есть ли необходимость постоянно обучать сотрудников службы информационной безопасности компании и, если есть, какие бюджетные средства для этого нужны?

13) Как управлять информационными рисками компании и какие инструментальные средства для этого необходимо задействовать?

Вопросы для самоконтроля

1. Какие определения термину «мониторинг» в раках системы информационной безопасности существует?
2. Поясните основные задачи мониторинга?
3. Какие контролируемые параметры аудита информационной безопасности могут быть использованы?
4. Опишите основные этапы аудита и мониторинга?

Литература: 1,2,3,4

4. Содержание самостоятельной работы

Самостоятельная работа студента по дисциплине включает в себя:

1. Изучение лекционного материала по конспекту лекций;
2. Изучение основной и дополнительной информации;
3. Подготовку к лабораторным занятиям;
4. Выполнение работы над курсовым проектом;
5. Выполнение индивидуальных заданий.

Объём часов, отводимый учебным планом для самостоятельной работы студента, составляет по очной форме обучения – 79 часа.

Индивидуальная работа организуется преподавателем для студентов на добровольной основе в следующих случаях: индивидуального графика обучения; углубленного изучения курса.

При обучении по индивидуальному графику студент должен выполнить все практические работы по темам курса. При углубленном изучении курса дополнительная программа составляется индивидуально с учетом вопросов для самостоятельного изучения. Кроме того, для более углубленного изучения дисциплины необходимо ознакомиться со следующими темами:

1. Оптимизация структуры управления службы защиты информации.
2. Мероприятия по контролю и мониторингу направлений деятельности службы защиты информации.
3. Оценка рисков при функционировании службы защиты информации.
4. Оценка эффективности работы службы защиты информации.
5. Технология управления службы защиты информации.
6. Порядок оформления документов, необходимых для получения лицензий, сертификатов, аттестатов в области защиты информации.
7. Разработка и применение методов локальной и комплексной автоматизации процессов деятельности службы защиты информации.
8. Интеграция службы защиты информации с подсистемами, обеспечивающими различные направления безопасности в организации.

Наименование разделов по темам	***Самостоятельное изучение разделов***
	Содержание
Введение. Основные понятия, связанные с функционированием службы защиты информации	Понятие об организации службы защиты информации. 1. Конспектирование источников литературы, электронных ресурсов в рамках основных понятий. 2. Поиск и обзор научных публикаций. 3. Проработка вопросов для самоконтроля, УМКД.
Место и роль службы защиты информации в системе защиты информации; задачи и функции службы	Понятие об организации службы защиты информации. 1. Конспектирование источников литературы, электронных ресурсов в рамках основных понятий. 2. Поиск и обзор научных публикаций. 3. Проработка вопросов для самоконтроля, УМКД.
Структура и штаты службы; подбор, расстановка и обучение сотрудников службы	Рассмотрение структуры, особенностей организации штатов службы защиты информации. 1. Конспектирование источников литературы, электронных ресурсов в рамках основных

	понятий. 2. Поиск и обзор научных публикаций. 3. Проработка вопросов для самоконтроля, УМКД.
Организационные основы и принципы деятельности службы	Организационная структура службы защиты информации для различных типов предприятий. 1. Конспектирование источников литературы, электронных ресурсов в рамках основных понятий. 2. Поиск и обзор научных публикаций. 3. Проработка вопросов для самоконтроля, УМКД.
Организация труда сотрудников службы	Особенности организации струда СЗИ 1. Конспектирование источников литературы, электронных ресурсов в рамках основных понятий. 2. Поиск и обзор научных публикаций. 3. Проработка вопросов для самоконтроля, УМКД.
Принципы, методы и технология управления службой	Изучение принципов управления СЗИ 1. Конспектирование источников литературы, электронных ресурсов в рамках основных понятий. 2. Поиск и обзор научных публикаций. 3. Проработка вопросов для самоконтроля, УМКД.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Показатель	*Требования ФГОС, %*	*Фактически, %*
Удельный вес активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги), %	Не менее 20 %	50 %

Технологии	*№ темы / тема лекции*	*№ практической работы / перечень*
Слайд-лекция	Введение. Основные понятия, связанные с функционированием службы защиты информации	
	Место и роль службы защиты информации в системе защиты информации; задачи и функции службы	
Лекция-дискуссия	Структура и штаты службы; подбор, расстановка и обучение сотрудников службы	Разработка организационно-правовых аспектов деятельности службы защиты информации
Индивидуальные задания на лабораторных работах.	Организационные основы и принципы деятельности службы	Разработка организационно-правовых аспектов деятельности службы защиты информации. Разработка организационной структуры службы защиты информации
Моделирование конкретных ситуаций	Организация труда сотрудников службы	Разработка модели системы защиты информации для службы защиты информации. Оценка производительности труда по результатам оптимизации процессов в службе защиты информации
Индивидуально-ориентированные задания на лабораторных и практических работах.	Принципы, методы и технология управления службой	Экспертная оценка мероприятий по защите информации в службе защиты информации. Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации

В процессе изучения дисциплины «Сопровождение и продвижение программного обеспечения отраслевой направленности» применяются следующие образовательные технологии:

- использование слайд-лекций на занятиях лекционного типа;
- разбор конкретных ситуаций.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УПРЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Для дисциплины «Организация и управление службой ЗИ» установлен один экзамен и предусмотрено промежуточное тестирование (в середине семестра).

При традиционной форме итогового контроля билет состоит из двух вопросов. Соответственно, при развернутых, верных ответах на два вопроса и приведенных примерах выставляется оценка «отлично». При недочетах и негрубых ошибках в ответе на один или два вопроса, студент получает оценку «хорошо». «Удовлетворительно» получают студенты, ответившие полно и верно на один вопрос, а на второй – очень слабо, или на два вопроса с существенными ошибками. «Неудовлетворительно» получают студенты, не ответившие ни на один из поставленных вопросов или допустившие грубые ошибки в ответах, демонстрирующие незнание вопроса.

При выставлении итоговой оценки учитываются результаты модульно-рейтинговой системы и защиты курсового проекта. По результатам проведенного экзамена выставляется оценка:

«отлично» – студентам, овладевшим целостными знаниями по дисциплине, активно работающим на лабораторных занятиях, постоянно и творчески выполняющим индивидуальные задания, свободно использующим знаниями, полученными в результате самостоятельной работы (86-100 баллов);

«хорошо» – студентам, владеющим знаниями по основным и дополнительным вопросам дисциплины, активно работающим на лабораторных занятиях, выполняющим различные индивидуальные задания, в достаточной мере разбирающимся в знаниях, полученных в ходе самостоятельной работы (70–85,9 баллов);

«удовлетворительно» – студентам, владеющим основными вопросами по тематике дисциплины, выполняющим лабораторные работы на достаточном уровне, в основном разбирающимся в темах дисциплины, вынесенных на самостоятельное изучение (50–74 баллов);

«не удовлетворительно» – студентам, не посещающим аудиторные занятия без уважительной причины, не владеющим основными вопросами изучаемой дисциплины, выполняющим лабораторные работы на низком уровне, слабо разбирающихся в вопросах, вынесенных на самостоятельное изучение (50 баллов менее).

Текущий и промежуточный контроль знаний осуществляется путем проведения тестирований, контрольных работ, отчетов по выполненным практическим работам. В связи с этим, для успешного освоения дисциплины студентам необходимо:

– регулярно посещать лекционные занятия;

– осуществлять регулярное и глубокое изучение лекционного материала, учебников и учебных пособий по дисциплине;

– активно работать на лабораторных занятиях;

– выступать с сообщениями по самостоятельно изученному материалу;

– участвовать с докладами на студенческих конференциях.

Текущий контроль знаний осуществляется путем выставления балльных оценок за выполнение тех или иных видов учебной работы (отчет по лабораторным работам, прохождение тестирования, контрольной работы и т.п.).

Промежуточный контроль знаний студентов осуществляется в форме межсессионной аттестации. Уровень знаний оценивается баллами, набранными студентами в контрольных точках. Балльная оценка соответствующих контрольных точек приводится в технологической карте дисциплины.

Итоговый контроль знаний по дисциплине проводится в форме письменного экзамена. Для подготовки к экзамену студенты используют приводимый ниже перечень вопросов для подготовки к экзамену. Вместе с тем, конкретная формулировка экзаменационных вопросов, не выходя за пределы изученных на аудиторных занятиях и в ходе самостоятельной работы, может отличаться от представленного перечня.

6.1. Примерные вопросы для подготовки к экзамену

1. Роль и место организационной защиты информации в системе комплексной защиты информации.

2. Основные термины и определения в области организационной защиты информации.

3. Задачи и функции, возлагаемые на руководителей и должностных лиц предприятия в решении задач по организационной защите информации.

3. Основные принципы и условия организационной защиты информации на предприятии.

4. Средства, используемые для обеспечения защиты конфиденциальной информации.

5. Стратегия обеспечения безопасности в организации. Подходы к построению Службы ЗИ

6. Организационно-планирующие документы по ЗИ, разрабатываемые в организации (на предприятии)

7. Положение «о подразделении по ЗИ организации». Назначение положения и модели его составления. Разработка и оформление положения

8. Должностные инструкции, сотрудника подразделения по ЗИ организации. Организация разработки должностной инструкции по ЗИ. Требования к проекту должностной инструкции сотрудника ЗИ. Особенности разработки нетипичных должностных инструкций

9. Понятия об организационной структуре управления подразделением по ЗИ. Требования, предъявляемые к ОСУ подразделением по ЗИ. Виды ОСУ подразделения по ЗИ

10. Система защиты государственной тайны на предприятии. Ее составные элементы.

11.Моделирование системы защиты информации (СЗИ). Виды моделей СЗИ. Архитектурное построение СЗИ.

12. Принципы отнесения сведений к государственной тайне и их засекречивания.

13. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.

14. Степени секретности сведений, составляющих государственную тайну, и грифы секретности их носителей.

15. Порядок отнесения сведений к государственной тайне.

16. Порядок засекречивания сведений и их носителей. Реквизиты носителей сведений, составляющих государственную тайну.

17. Перечень сведений, отнесенных к государственной тайне, порядок и особенности его формирования. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

18. Основания и порядок рассекречивания сведений, составляющих государственную тайну, и их носителей.

19. Функции в области рассекречивания сведений, составляющих государственную тайну, возлагаемые на Межведомственную комиссию по защите государственной тайны.

20. Порядок исполнения запросов граждан, предприятий, учреждений, организаций и органов государственной власти Российской Федерации о рассекречивании сведений, составляющих государственную тайну.

21. Основные положения допуска должностных лиц и граждан к сведениям, составляющим государственную тайну.

22. Порядок оформления (переоформления) допуска должностных лиц и граждан к государственной тайне.

23. Формы допуска. Особый порядок допуска к государственной тайне. Условия прекращения допуска к государственной тайне.

24. Обязанности лиц, допущенных к сведениям, составляющим государственную тайну. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.

25. Основания для отказа должностному лицу и гражданину в допуске к государственной тайне.

26. Понятие внутриобъектового режима на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима.

27. Роль и место внутриобъектового режима на предприятии в общей системе защиты конфиденциальной информации.

28. Силы и средства, используемые при организации внутриобъектового режима на предприятии.

31. Цели и задачи пропускного режима на предприятии. Основные понятия, используемые при его организации и обеспечении.

29. Принципы организации пропускного режима на предприятии. Основные элементы системы организации пропускного режима, используемые силы и средства.

30. Особенности организации пропускного режима на предприятиях, имеющих особый статус. Ответственность за нарушение пропускного режима.

31. Планирование мероприятий по защите сведений конфиденциального характера при подготовке совещаний (заседаний, конференций, симпозиумов), в ходе которых предполагается обсуждение вопросов, содержащих такие сведения.

32. Работа по исключению утечки сведений и информации конфиденциального характера.

33. Цели и задачи службы охраны предприятий, выполняющих работы с конфиденциальной информацией.

34. Основные способы организации и осуществления охраны предприятий, выполняющих работы с конфиденциальной информацией.

35. Основные направления деятельности должностных лиц предприятия по организации его охраны. Особенности охраны предприятий, имеющий особый статус.

36. Особенности организации охраны предприятий, выполняющих работы с конфиденциальной информацией, подразделениями вневедомственной охраны при органах внутренних дел МВД России и частными предприятиями, выполняющими функции защиты информации.

37. Основные положения организации защиты конфиденциальной информации в ходе подготовки и командирования сотрудников предприятия (организации) в органы государственной власти, на другие предприятия и в организации.

38. Порядок и последовательность оформления необходимых документов о командировании сотрудников предприятия в органы государственной власти, на другие предприятия (в организации).

39. Какие типовые организационные структуры можно выделить в рамках государственной системы защиты информации?

40. Какие услуги организационно-технологического характера предлагаются специализированными предприятиями в системе защиты информации?

41. Какие основные функции выполняют сертификационно-испытательные центры и лаборатории в области обеспечения и защиты информации?

42. Перечислите основные функции, выполняемые

6.2. Примерные тестовые задания

Предложенные тестовые задания можно использовать для формирования тестов для текущего, промежуточного контроля, а также для организации контроля в дистанционном образовании по дисциплине «Организация и управление службой ЗИ».

1. Меры защиты информационной безопаснсоти направлены на защиту от:

а) нанесения неприемлемого ущерба;

б) нанесения любого ущерба;

в) вандализма.

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

а) доступность;
б) целостность;
в) конфиденциальность;
г) правдивое отражение действительности.

3. Что такое защита информации?
а) защита от несанкционированного доступа к информации;
б) выпуск бронированных упаковок для дисков;
в) комплекс мероприятий, направленных на обеспечение информационной безопасности.

4. Что понимается под информационной безопасностью?
а) защита здоровья персонала;
б) защита отнанесения неприемлемого ущерба субъектам информационных отношений;
в) обеспечение информационной независимости России.

5. Самыми опасными угрозами являются:
а) непреднамеренные ошибки штатных сотрудников;
б) вирусные инфекции;
в) атаки хакеров.

6. Дублирование сообщений является угрозой:
а) доступности;
б) куонфиденциальности;
в) целостности.

7. Агрессивное потребление ресурсов является угрозой:
а) доступности;
б) конфиденциальности;
в) целостности.

8. Согласно Закону “Об информации, информатизации и защите информации”, персональные данные – это:
а) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
б) данные, хранящиеся в персональном компьютере;
в) данные, находящиеся в чьей-либо персональной собственности.

9. Действия Закона “О лицензировании отдельных видов деятельности” не распространяется на:
а) деятельность по технической защите конфиденциальной информации;
б) образовательную деятельность в области защиты информации;
в) предоставление услуг в области шифрования информации.

10. Главная цель мер по защите информации, предпринимаемых на административном уровне:
а) сформировать программу безопасности и обеспечить её выполнение;
б) выполнить положения действующего законодательства;
в) отчитаться перед вышестоящими инстанциями.

11. В число целей политики безопасности верхнего уровня входит:
а) решение сформировать или пересмотреть комплексную программу безопасности;
б) обеспечение базы для соблюдения законов и правил;
в) обеспечение конфиденциальности почтовых сообщений.

12. В число этапов жизненногоцикла информационного сервиса входят:
а) закупка;
б) продажа;
в) выведение из эксплуатации.

13. Политика безопасности:
а) фиксирует правила разграничения доступа;

б) отражает подход организации к защите своих информационных активов;

в) описывает способы защиты руководства организации.

14. В число этапов процесса планирования восстановительных работ после реализации угроз входят:

а) выявление критически важных функций организации;

б) определения перечня возможных аварий;

в) проведение тестовых аварий.

15. В число принципов физической защиты входят:

а) беспощадный отпор;

б) непрерывность защиты в пространстве и времени;

в) минимизация защитных средств.

16. Мониторинг, протоколирование и аудит могут использоваться для:

а) предупреждения нарушений ИБ;

б) обнаружение нарушений;

в) восстановление режима ИБ.

17. В число основных принципов архитектурной безопасности входят:

а) применение наиболее передовых технических решений;

б) применение простых апробированных решений;

в) сочетание простых и сложных защитных средств.

18. Контроль целостности может использоваться для:

а) предупреждения нарушений информационной безопасности;

б) обнаружения нарушений;

в) локализации последствий нарушений.

19. Обеспечение высокой доступности можно ограничить:

а) критически важными серверами;

б) сетевым оборудованием;

в) всей цепочкой от пользователей до серверов.

20. Некотрые авторы включают в число основных аспектов безопасности подотчетность. На Ваш взгляд, это:

а) правильно, потому что без подотчетности не может быть безопасности;

б) неправильно, потому что подотчетность – не цель, а средство достижения безопасности;

в) не имеет значения, потому что все это словесная эквилибристика, далекая от реальной безопасности.

21. Предметная область «Защита информации» согласно ГОСТ Р 50922—96 – это:

а) деятельность (процесс), направленная на предотвращение утечки защищаемой информации;

б) специальное устройство для защиты информации;

в) производственное объединение.

22. Служба защиты информации (СЗИ) – это:

а) государственное учреждение по защите информации;

б) специализаированная организация;

в) это самостоятельное структурное подразделение в рамках деятельности организации, тесно связана со службами охраны и объектового режима, составляет основу всей системы обеспечения информационной безопасности.

23. Что нельзя отнести к функциям, выполняемым службой защиты информации:

а) финансовое обеспечение деятельности организации;

б) организация обучения персонала правилам соблюдения и поддержания информационной безопасной деятельности предприятия;

в) материально-техническое и технологическое обеспечение информационной безопасности на предприятии.

24. Что можно отнести к функциям управления подразделением по защите информации?

а) планирование,

б) контроль;

в) разработка программного обеспечения.

25. Функция управления, связанная с определением целей управления подразделением по защите информации, поиском методов, необходимых для достижения поставленных целей на защиту информации и определением системы показателей, определяющих эффективность применения методов для достижения поставленных целей – это:

a) Организация деятельности подразделения по защите информации;

b) Контроль деятельности подразделения по защите информации;

c) Планирование деятельности подразделения по защите информации.

26. К организационным задачам и функциям службы защиты информации не относится:

a) разработка и проектов защиты для каждого вида безопасности их реализация приемки и контроль за постоянной работоспособности;

b) организация проведения совместно с другими подразделениями мероприятий в отношении конкурентов, взаимодействия с правоохранительными органами;

c) оказание управленческих воздействий на создание/поддержку своевременной реорганизацию структуры управления безопасности предприятия.

27. Управление качеством работы подразделения по защите информации и затратами на защиту информации являются функциями управления:

a) результатами защиты информации;

b) процессами защиты информации;

c) ресурсами, выделяемыми на защиту информации.

28. К факторам, влияющим на организацию службы ЗИ не относится:

a) финансовые возможности предприятия;

b) решения акционеров предприятия;

c) масштабы предприятия.

29. Отраслевое и функциональное, структурное подразделение по ЗИ, осуществляющее исполнительные и организационно-распорядительные функции, отнесённые к его введенью в пределах одного из направлений деятельности по ЗИ – это:

a) Служба защиты информации;

b) Отдел защиты информации;

c) Сектор/группа по защите информации.

30. Такие недостатки как низкая оперативность решения, степень доверия и ответственности к сторонней организации характерны для:

b) Создания службы ЗИ, минимизированной по исполняемым функциям;

c) Создания службы ЗИ с ограниченными функциями;

d) Создания полноценной службы по исполняемым функциям.

31. Лаборатория - это:

a) централизованно управляемая, совокупность структурных подразделений по ЗИ объединённая общими целями, функциями и объектами управления;

b) структурное подразделение по ЗИ, которое осуществляет исполнительные и организационно-распорядительные функции по исследованию вопросов ЗИ, возможностей реализации, средств и технологий защиты информации;

c) структурное подразделение отдела/отделения по ЗИ, осуществляющее исполнительную деятельность, возглавляемое главным специалистом или старшим инженером, и объединяющее 2-х или более специалистов по ЗИ, инженеров, техников в одном тематическом направлении деятельности отдела/отделения.

32. На чем должно базироваться правовое обеспечение информационной безопасности?

a) соблюдение принципов законности;

b) комплексности и индивидуальности;

c) системности подходов;

d) балансе интересов в информационной сфере;

e) взаимодействии и координации.

33. Назовите методы управления подразделением по ЗИ

a) экономические;
b) правовые;
c) юридические;
d) социально-психологические;
e) принудительные.

34. Через какие стимулы и мотивы воздействуют социально-психологические методы управления подразделением по ЗИ?

a) увеличение заработной платы;
b) развитие социальных потребностей и интересов;
c) развитие межличностных коммуникаций.

35. Каковы требования к технологии управления безопасностью?

a) соответствие современному уровню развития информационных технологий;
b) выделение максимально возможных средств на защиту информации;
c) наличие обособленных субъектов в информационной системе.

36. Какая проблема является основной, с точки зрения соблюдения политики безопасности на предприятии?

a) недостаточно грамотное построение пропускного режима
b) недостаточно грамотное формулирование должностных инструкций
c) недостаточное обучение персонала

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности [Текст] : учеб. пособие / А. А. Анисимов. - М. : БИНОМ. Лаб. знаний, 2010. - 175 с. - (Основы информационных технологий)
2. Горбатов, В.С. Введение в информационную безопасность [Электронный ресурс] : учеб. пособие для вузов / под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2011. - 288 с. - Режим доступа: http://www.iprbookshop.ru/11979.html
3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению "Информатика и вычисл. техника" / В. Ф. Шаньгин. - М. : ФОРУМ [и др.], 2013. - 592 с. - (Высшее образование) - Режим доступа: http://znanium.com/bookread.php?book=402686
4. Шелупанова, А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учеб. пособие для вузов по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" / под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. - М. : Горячая линия - Телеком, 2012. - 550 с. - Режим доступа: http://www.iprbookshop.ru/11978.html

Дополнительная литература

5. Абдикеев, Н. Б. Корпоративные информационные системы управления [Текст] : учебник / Н. М. Абдикеев, Н. Б. Завьялова, А. Д. Киселев [и др.] под науч. ред. Н. М. Абдикеева, О. В. Китовой. - М. : Инфра-М, 2010. - 464 с. : ил., табл. - (Высшее образование)
6. Александров, Д. В. Методы и модели информационного менеджмента [Текст] : учеб. пособие для вузов по специальности "Приклад. информатика (по обл.)" и экон. специальностям / Д. В. Александров, А. В. Костров, Р. И. Макаров [и др.] под ред. А. В. Кострова. - М. : Финансы и статистика, 2009. - 335 с. : ил.
7. Благодатин, А. А. Финансовый словарь [Текст] / А. А. Благодатин, Л. Ш. Лозовский, Б. А. Райзберг. - М. : ИНФРА-М, 2009. - 377 с. - (Библиотека малых словарей "ИНФРА-М")
8. Бочкарев, А. И. Фундаментальные основы защиты информации [Текст] : лаб. практикум для студентов специальности "Орг. и технология защиты информ." и др. специальностей и направлений / Поволж. гос. ун-т сервиса (ПВГУС), Каф. "Соврем. естествознание" ; сост.: А. И. Бочкарев, Т. С. Бочкарева, В. В. Смоленский. - Тольятти : ПВГУС, 2009. - 103 с.
9. Вдовенко, Л. А. Информационная система предприятия [Текст] : учеб. пособие для вузов, аспирантов, магистров экон. вузов / Л. А. Вдовенко. - М. : Вузов. учеб. [и др.], 2010. - 236 с. : ил. - (Вузовский учебник)
10. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов по специальностям "Орг. и технология защиты информ.", "Комплекс. защита объектов информатизации" / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 412 с. - (Высшее профессиональное образование. Информационная безопасность)
11. Ивасенко, А. Г. Информационные технологии в экономике и управлении [Электронный ресурс] : учеб. пособие для вузов по специальностям "Приклад. информатика (по обл.)", "Менеджмент орг.", "Гос. и муницип. упр." / А. Г. Ивасенко, А. Ю. Гридасов, В. А. Павленко. - М. : КноРус, 2010. - 154 с. - Режим доступа: http://www.book.ru/view/266721/2
12. Калянов, Г. Н. Консалтинг: от бизнес-стратегии к корпоративной информационно-управляющей системе [Текст] : учеб. для вузов по специальности "Приклад. информати-

ка (по областям)" и др. экон. специальностям / Г. Н. Калянов. - М. : Горячая линия - Телеком, 2011. - 210 с. - (Учебник для высших учебных заведений)
13. Клейменов, С. А. Информационная безопасность и защита информации [Текст] : учеб. пособие для вузов по специальности "Информ. системы и технологии" / под ред. С. А. Клейменова. - М. : Академия, 2011. - 336 с. - (Высшее профессиональное образование. Информатика и вычислительная техника)
14. Малышева, Е. Ю. Системы автоматизированной обработки экономической информации [Текст] : учеб. пособие для вузов по специальности "Приклад. информатика (по обл.)" и др. экон. специальностям / Е. Ю. Малышева, С. М. БобровскийПоволж. гос. ун-т сервиса (ПВГУС). - Тольятти : ПВГУС, 2010. - 103 с. : ил.
15. Райзберг, Б. А. Прикладная теория управления экономическими системами [Текст] : учеб.-метод. пособие / Б. А. РайзбергМоск. психол.-соц. ин-т. - М. : МПСИ, 2011. - 460 с. : табл.
16. Титоренко, Г. А. Информационные системы в экономике[Текст] : учеб. для вузов по специальностям "Финансы и кредит", "Бухгалт. учет, анализ и аудит" / под ред. Г. А. Титоренко. - М. : ЮНИТИ-ДАНА, 2009. - 463 с.
17. Титоренко, Г. А. Информационные системы и технологии управления [Текст] : учеб. для вузов по специальности "Финансы и кредит", "Бухгалт. учет, анализ и аудит", по направлениям "Менеджмент" и "Экономика" / Г. А. Титоренко, И. А. Коноплева, В. И. Суворова [и др.] под ред. Г. А. Титоренко. - М. : ЮНИТИ-ДАНА, 2013. - 591 с. : табл. - (Золотой фонд российских учебников)

Программное обеспечение современных информационно-коммуникационных технологий и Интернет-ресурсы

Для ведения данной дисциплины необходимо следующее программное обеспечение: Операционная система Microsoft Windows, MS Office, Информационно-справочные системы: Консультант-Плюс, Гарант.

1. citforum.ru [Электронный ресурс] : журнал. – Режим доступа: http://www.citforum.ru. – Загл. с экрана.
2. Экономическая безопасность [Электронный ресурс] : журнал. – Режим доступа: http://ru.wikipedia.org/wiki - Загл. с экрана.

8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПРЕПОДАВАТЕЛЮ

Тематика лекций и практических занятий по дисциплине «Организация и управление службой ЗИ» соответствует требованиям ФГОС по подготовке в области организации и защиты информации.

Основными формами обучения студентов являются аудиторные занятия, включающие лекции и выполнение практических работ, а также выполнение предусмотренных рабочей учебной программой видов самостоятельной работы.

Средства обучения, применяемые при преподавании дисциплины «Организация и управление службой ЗИ» можно разделить на следующие группы:

- технические (проектор, ПК)
- программные (программное обеспечение – см раздел 5)
- информационные (литература, периодические издания, методические указания как в печатной так и в электронной форме)

Методы обучения. В отечественной практике предложено несколько признаков классификации методов обучения. По источнику передачи и восприятия учебной деятельности в процессе обучения данной дисциплине применяются следующие:

- словесный (чтение лекции);
- наглядный (использование проектора, доски);
- практический (деятельностный) (выполнение практических работ).

По степени самостоятельности мышления можно выделить следующие: репродуктивные, проблемно-поисковые.

Дополнительно к этим методам следует добавить методы, обеспечивающие целевое назначение основных (традиционных):

- методы формирования познавательных интересов у студентов (дискуссии во время занятий, защиты рефератов);
- метод самостоятельных работ (написание рефератов и чтение доп. литературы)

При подготовке к лекциям важно учитывать принципы дифференцированного подхода к студентам. Проведение лекций должно осуществляться с учетом активных форм обучения на основе использования мультимедийных материалов и презентаций (слайдов). Для наглядного представления содержания лекций необходима демонстрация моделей, схем, таблиц. В заключение лекции указываются дополнительные источники информации, в том числе книги, электронные ресурсы, которые содержат интересный материал по теории и практике системного анализа, не вошедший в основной курс.

Выполнение практических работ позволяет закрепить полученные теоретические знания и проверить остаточные знания по ранее изученным дисциплинам, которые будут необходимы в дальнейшем обучении. При выполнении практических работ необходимо обеспечить возможность использования студентами современных информационных технологий.

Проведение преподавателем курса практических работ включает:

- информационно-справочное обеспечение выполнения заданий;
- учет степени подготовленности при выдаче информации и дифференцированный подход;
- управление процессом выполнения практических работ;
- контроль результатов, в процессе которого каждому студенту указывается на допущенные в работе ошибки. Результатом контроля является балльная оценка работы (согласно технологической карте дисциплины).

Оценка полученных в ходе изучения дисциплины знаний происходит во время приема практических работ, обсуждения докладов (лекций проводимых под руководством преподавателя). Промежуточный контроль знаний студентов осуществляется в форме межсессионной аттестации. Уровень знаний оценивается баллами, набранными студентами в контрольных точках. Балльная оценка соответствующих контрольных точек приводится в технологической карте дисциплины. По окончании изучения дисциплины проводится итоговый контроль – экзамен.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ

Организация учебного процесса должна выполняться с учетом требований, изложенных в федеральном государственном образовательном стандарте.

Изучение дисциплины «Организация и управление службой ЗИ» требует:

- прослушивания лекций преподавателя и дополнительное самостоятельное изучение разделов, тем;
- выполнения и защиты практических работ в аудитории;
- подготовку рефератов (в качестве дополнительного задания).

Лабораторные работы выполняются индивидуально. По итогам выполнения работы предоставляется один экземпляр отчета.

Внеаудиторная самостоятельная работа студентов представляет собой вид занятий, которые каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает:

- самостоятельное изучение разделов дисциплины;
- подготовку к практическим работам;
- подготовку рефератов, сообщений и докладов.

Промежуточный контроль знаний студентов осуществляется в форме межсессионной аттестации. Уровень знаний оценивается баллами, набранными студентами в контрольных точках. Балльная оценка соответствующих контрольных точек приводится в технологической карте дисциплины (см. приложение 1).

9.1. Методические указания и темы для выполнения курсовых работ

Цели, задачи и основное содержание курсовой работы

При освоении дисциплины «Организация и управление службой защиты информации» важнейшей формой контроля самостоятельной работы студента является выполнение и защита курсового проекта.

Цель написания курсового проекта: научиться применять полученные теоретические знания для решения конкретных задач. Теоретические знания – это изученный понятийный аппарат дисциплины, методы системного анализа, функционального моделирования, методики разработки организационно-правового, технического, программно-аппаратного обеспечения функционирования службы защиты информации. Конкретные задачи, поставленные перед автором курсового проекта, зависят от темы.

В случае успешного выполнения курсового проекта студент может быть рекомендован для участия в научно-практических конференциях и конкурсах научных работ.

Задачи написания курсового проекта сводятся к тому, что студент должен научиться:

- логично, последовательно, с соблюдением требований научного стиля излагать материал курсового проекта;
- обобщать сведения, полученные из учебной, научной литературы, периодических изданий и официальных Интернет-ресурсов;
- выбирать методы исследования и анализа систем защиты информации в рамках деятельности конкретной организации в целом в соответствии с типом системы определять методику анализа;
- проводить анализ целей и функций, задач управления службой защиты информации, в том числе определять цель системы и строить структуры целей и функций;
- строить математические, графовые модели структуры управления СЗИ;
- использовать методы аудита и мониторинга СЗИ, разработки критериев оценки деятельности СЗИ, а также методов экспертной оценки;
- анализировать процессы и структуры управления системами защиты информации и вносить предложения по их совершенствованию.

Таким образом, в ходе выполнения курсового проекта студент приобретает опыт выработки методики формирования организационно-правового обеспечения службы защиты

информации на основе системного анализа с использованием возможностей вычислительной техники и программного обеспечения, а также изучает один из методов исследования и моделирования организационно-управленческих аспектов службы защиты информации.

Структура и объем курсовой работы

Общий объем курсового проекта – 30-35 страниц. Курсовой проект должен иметь обязательные составные части, располагаемые в последовательности:

- титульный лист;
- содержание;
- введение;
- основная часть;
- заключение;
- библиографический список;
- приложения.

Дополнительно прилагаются задание на курсовой проект и бланк рецензии. Они размещаются после титульного листа и не нумеруются.

Титульный лист оформляется по установленной форме.

Задание на курсовой проект выдается руководителем по установленной форме и утверждается заведующим кафедрой.

Рецензия. Бланк рецензии оформляется по установленной форме. Рецензию пишет руководитель после представления курсового проекта на проверку.

Содержание (1-2 страницы). Содержание отражает последовательность составных частей курсового проекта: введение, названия глав и параграфов, заключение, библиографический список, приложения. В содержании указывается название пункта и номер страницы, с которой начинается его изложение. При этом главы и параграфы нумеруются арабскими цифрами, остальные пункты не нумеруются.

Введение (3-4 страницы). Содержит обоснование актуальности темы, постановку проблемы и отражение состояния вопроса. Обязательно четко выделить цель и задачи курсового проекта. Формулировка цели работы является логическим продолжением сформулированной проблемы, актуальности темы и должна быть созвучна наименованию темы. Главной целью научной деятельности, а курсового проекта есть форма научной работы, является получение знаний о реальности. Обычно цель формулируется с помощью отглагольных существительных (получение, анализ, разработка и т.п.) и должна ёмко отражать то, что собирается достичь исследователь в ходе выполнения работы.

Для достижения поставленной цели необходимо сформулировать конкретные задачи курсового проекта. Это делается в форме перечисления (изучить..., установить..., выявить..., разработать..., проанализировать..., сделать выводы… и т. д.). Поскольку из формулировок задач исследования составляются обычно заголовки параграфов работы, то задачи рекомендуется формулировать более тщательно.

Также необходимо выделить объект исследования (например, указывается наименование предприятия) и кратко указать материалы и методы, используемые в процессе исследования.

Если курсовой проект имеет научный характер, предполагает достижение уровня научной новизны, то авторам рекомендуется обратиться к литературе по методологии научного творчества (например, [30], [45]).

Основная часть (22-25 страниц). Основная часть состоит из двух глав. В первой главе излагаются теоретические аспекты темы, проводятся анализ предприятия или организации с учетом особенностей организации системы защиты информации, во второй главе – преимущественно разработка решений поставленной проблемы, выбор оптимального варианта решения и формулирование предложений по его внедрению.

Заключение (2-3 страницы). В заключении приводятся самостоятельные выводы о проделанной работе и полученных результатах исследования. Выводы должны быть краткими и аргументированными, рекомендации – конкретными и сопровождаться оценкой от их внедрения в практику.

Библиографический список. Каждая позиция в библиографическом списке должна быть оформлена в соответствии с требованиями ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». При оформлении курсового проекта используется алфавитный способ группировки библиографических описаний.

Требования к составу списка:

- общее количество источников - не менее 20 (из них не менее 15 источников, выпущенных после 2006 года);
- диссертаций, авторефератов диссертаций, монографий – не менее двух;
- статей из периодических изданий, сборников конференций – не менее пяти.

Рекомендуется использовать нормативно-правовые документы, если они соответствуют теме курсового проекта и необходимы для достижения поставленных задач. Допускается включать в библиографический список электронные издания, Интернет-ресурсы, если они содержат статистическую, аналитическую, обзорную информацию, являются официальными сайтами организаций, предприятий, учреждений, а не представляют собой базы рефератов, курсовых и дипломных работ.

Приложения. Содержат дополнительный иллюстративный, табличный материал, документы (или их фрагменты), описание порядка реализации методов системного анализа, не вошедшие в основную часть работы. Объем приложений не ограничен и не включается в объем курсового проекта (30-35 страниц). Содержание приложений должно быть оправдано темой, целью и задачами исследования.

Общие требования к оформлению курсовой работы

Текст работы выполняется машинописным способом на стандартных листах формата А4 (210х297) без рамки, нелинованных, на одной стороне листа с соблюдением следующих размеров полей: верхнее – 20 мм, правое – 10 мм, левое – 30 мм, нижнее – 20 мм. Абзацный отступ – 1,25 см. Шрифт Times New Roman, размер шрифта 12, межстрочный интервал – полуторный, выравнивание – по ширине. Заголовки первого уровня (содержание, введение, названия глав, заключение, библиографический список, приложения) оформляются шрифтом Times New Roman, размер - 14, начертание – полужирными, прописными буквами, выравнивание – по центру. Заголовки второго уровня (названия параграфов, названия приложений) оформляются шрифтом Times New Roman, размер - 12, начертание – полужирный курсив, строчными, выравнивание – по центру. Подробнее в [9].

Главы (разделы) и параграфы работы нумеруются арабскими цифрами. При этом номер параграфа состоит из двух частей, например, 1.2. (второй параграф первой главы). В конце заголовка точка не ставится. Каждая новая глава, как и введение, заключение, библиографический список, приложение, начинается с новой страницы. Расстояние между названием параграфа и последующим текстом должно быть равно одному пробелу (пустой строке). Такое же расстояние выдерживается между заголовками раздела и параграфа. Между строчками в заголовках параграфов, таблиц, подписях к рисункам, в сносках внизу страницы выдерживается одинарный интервал.

Подписи к рисункам оформляются под рисунком (шрифт Times New Roman, размер - 12, полужирный, выравнивание – по центру). При этом подпись состоит из номера и названия рисунка (например, Рис.2.1.Подпись к рисунку – первый рисунок во второй главе). Точка в конце подписи не ставится.

Таблицы должны иметь названия, все графы (колонки) в таблице нумеруются. К каждой таблице дается примечание со ссылкой на источник, откуда взяты цифровые данные, если они заимствованы. Таблицы, как и рисунки, нумеруются последовательно арабскими цифрами в пределах одной главы. Надпись «Таблица» с указанием ее номера (например, Таблица 2.3, т.е. третья таблица во второй главе) помещается над заголовком таблицы и выравнивается по правому краю. После этого на следующей строке по центру располагается заголовок таблицы (Times New Roman, 12, полужирный). При переносе таблицы на следующую страницу заголовок таблицы следует повторить и над ней поместить слова «Продолжение табл.А.В.» (А – номер главы, В – номер таблицы). Если шапка таблицы громоздка, до-

пускается ее не повторять. В этом случае пронумеровываются графы, а их нумерацию повторяют на следующей странице. Таблицы, приведенные в приложении, нумеруются как приложения. Дробные числа желательно приводить в виде десятичных дробей. В графах таблиц нельзя оставлять свободные места. Если данные отсутствуют, то следует поставить тире или написать «нет».

Ссылки на таблицы, рисунки, приложения даются в тексте (см.табл.1; см.рис.2; см.прил.3). Рисунки, таблицы, приложения должны дополнять основную текстовую часть курсовой работы, способствовать раскрытию темы.

Библиографический список оформляется в соответствии с требованиями ГОСТ 7.1-2003. Все приводимые в работе цитаты, заимствования и цифровые данные, полученные другими авторами, должны иметь ссылку на источник. Ссылки приводятся внутри текста. После упоминания источника или цитаты из него проставляется заключенный в квадратные скобки порядковый номер, под которым этот источник значится в библиографическом списке, и номер страницы. Например, [20, с.12], [6, с.290-291].

Нумерация страниц курсового проекта сквозная, включая библиографический список и приложение. Первой страницей, которая не нумеруется, является титульный лист, второй - содержание работы и т.д. Номера страниц проставляются арабскими цифрами в середине верхней части листа, начиная со второй страницы. Задание на курсовую работу, рецензия в число страниц не включаются.

В тексте желательно избегать сложных и громоздких предложений. Не принято писать в работе от первого лица единственного числа. Желательно использовать безличные предложения или излагать материал от первого лица множественного числа (например, «по нашему мнению», «нами был проведен анализ…»). Допускается использовать только общепринятые аббревиатуры и сокращения.

Последовательность выполнения курсовой работы

Выбор темы осуществляется студентом самостоятельно по согласованию с руководителем курсового проекта и студенческой группой. Основные критерии выбора темы: темы не должны повторяться в пределах студенческой группы (потока, если группы малочисленные); тема должна соответствовать интересам студента и наличию у него возможностей для сбора фактического материала. Так, например, если студента интересует деятельность предприятий по разработке и обслуживанию программного обеспечения, то рекомендуется выбрать тему по анализу СЗИ предприятия в этой сфере.

Наконец, студенту, заинтересованному в научном творчестве, решении относительно нестандартных задач, можно порекомендовать выбрать тему научного типа.

После выбора темы оформляется задание на выполнение курсового проекта.

Следующий этап – сбор и обработка материала. При работе над темой первого типа студенту рекомендуется обратиться к фактическому материалу по организационно-правовому обеспечению системы защиты информации выбранного предприятия, познакомиться с его деятельность, организационной структурой, функциями персонала, технологическими процессами. Также необходимо провести анализ аналогов, то есть определить, как выявленную проблему решают другие предприятия, действующие в этой отрасли – российские и зарубежные. В этой работе важно использовать методы системного анализа. Перейдя ко второй части работы, требуется выработать варианты решения выявленной проблемы.

Если студеносящим выполняет проект с учетом научно-исследовательскийт характера, важно подойти максимально творчески. Материалом для аналитической части курсового проекта послужат монографии, диссертации, статьи в рецензируемых научных журналах, аналитическая и статистическая информация, обзоры, размещенные на официальных сайтах. Во второй части работы студент излагает собственные идеи по решению выявленных проблем, увязывая их с достижениями современной науки и техники. Важно выделить новизну предлагаемого решения (теоретического, практического характера).

Полученные данные сопровождаются комментариями, формируется библиографический список, обязательно даются ссылки на источники по тексту работы. Выполненный, оформленный по требованиям курсовой проект студент в срок, предусмотренный графиком,

сдает на кафедру для рецензирования. Качество курсового проекта оценивается руководителем с учетом теоретического и практического содержания, достижения ее цели и задач.

При проверке курсовых проектов, представляемых на рецензию, отмечают недочеты: низкий теоретический уровень работы, частичное или полное заимствование текста, грамматические и стилистические ошибки, отсутствие какой-либо составной части курсового проекта, неправильное оформление и другие. Приведенные и возможные другие недостатки курсового проекта влекут за собой возврат работы на повторное выполнение или доработку.

Курсовой проект, получивший отрицательную рецензию, выполняется студентом повторно с учетом замечаний. При сдаче вновь выполненной работы следует приложить к ней не принятую к защите работу и рецензию на нее. Допущенный к защите курсовой проект остается на кафедре до начала зачетно-экзаменационной сессии. Во время сессии проект выдается студенту и после защиты возвращается на кафедру.

Одним из условий успешной защиты является высокий уровень самостоятельности подготовленного курсового проекта. Поэтому каждая работа должна пройти через систему AntiPlagiat.ru. Интернет-сервис AntiPlagiat.ru предлагает набор услуг, в совокупности реализующих технологию проверки текстовых документов на наличие заимствований из общедоступных сетевых источников. Проверка через систему AntiPlagiat.ru может быть выполнена студентом самостоятельно с предоставлением преподавателю печатной копии краткого отчета и электронной копии полного отчета, выданного автоматизированной системой. Режим доступа к Интернет-сервису: www.antiplagiat.ru.

Процедура защиты курсового проекта студентами дневного и заочного отделения включает:

1) подготовку презентации (10-15 слайдов) в формате Microsoft Power Point и текста доклада (5-6 минут); обязательные слайды: тема работы, цель и задачи работы, выводы и рекомендации (полученные результаты);
2) выступление в день защиты курсового проекта с докладом, ответы на вопросы преподавателя и аудитории.

Примерный перечень тем курсовых работ

1. Разработка организационно-правовых аспектов деятельности системы комплексной защиты информации (на примере конкретной организации)
2. Разработка системы учета и контроля поступивших конфиденциальных документов в комплексной системе защиты информации
3. Характеристика организационных и технических мер в комплексной службе защиты информации в государственных структурах
4. Разработка концептуальных основ функционирования систем безопасности предпринимательской деятельности (на примере проектирования конкретной системы)
5. Разработка политики безопасности и принципов управления службой информационной безопасности предприятия
6. Теория и практика организации защиты информационных систем
7. Разработка службы информационной безопасности для вечурного фонда
8. Разработка интегрированной системы защиты в рамках службы защиты информации (на примере конкретной организации)
9. Модернизация службы защиты информации (на примере конкретной организации)
10. Разработка политики безопасности при эксплуатации и сопровождении ИС с целью обеспечения сохранности конфиденциальной информации

Исходные данные для выполнения курсовой работы

Приступая к выполнению курсового проекта, студент руководствуется индивидуальным заданием, материалами, собранными на предприятии, данными, опубликованными в научной литературе, официальных отчетах, обзорах, релизах. В списке рекомендуемой литературы приведены книги и источники, которые могут быть полезны при написании курсовых

работ практически по всем темам. Разумеется, база учебной, научной литературы, официальных изданий должна быть расширена студентом индивидуально, в зависимости от тематики работы.

Индивидуальное задание оформляется по установленной форме, но может быть дополнено руководителем в ходе консультаций по курсовому проекту.