Основы системы информационной безопасности

Вводная часть

В ходе данного занятия будут изучены понятия «концепции», «политики» и «системы информационной безопасности» и их содержание.

Актуальность данного занятия заключается в том, что организации и предприятия любого типа:

- собирают, обрабатывают, хранят и передают большое количество информации;
- понимают, что информация и относящиеся к ней процессы, системы, сети и персонал являются важными ресурсами для решения задач, стоящих перед организацией;
- сталкиваются с рядом рисков, которые могут оказывать воздействие на функционирование активов организации;
- ослабляют риски, осуществляя управление информационной безопасностью.

Мы уже неоднократно сталкивались с термином активы организации и неоднократно еще будем его упоминать. Поэтому кратко рассмотрим содержание данного термина.

Активы организации – это все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

К активам организации могут относиться:

- информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);
- ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);
- процессы (технологические, информационные и пр.).

Вся информация, хранящаяся и обрабатывающаяся в организации, является объектом угроз, атак, ошибок, воздействия стихии и т.д. Термин «информационная безопасность» относится к информации, которую рассматривают как актив, у которого есть ценность, требующая соответствующей защиты, например, от потери доступности, конфиденциальности и целостности. Создание системы информационной безопасности направлено на обеспечение доступности, конфиденциальности и целостности активов организации (предприятия), что значительно повышает эффективность работы организации или предприятия при достижении своих целей.

В ходе занятия будут рассмотрены следующие учебные вопросы:

1. Понятие «концепции» и «политики» информационной безопасности.
2. Цель и задачи системы информационной безопасности.
3. Применение системного подхода к созданию системы информационной безопасности.

Первый учебный вопрос: «Понятие концепции и политики информационной безопасности»

Защита информационных активов посредством определения, достижения, поддержания и улучшения информационной безопасности очень важна для того, чтобы позволить организации достигать своей цели, а также поддерживать и повышать уровень соответствия законодательству и репутации. Эти скоординированные действия, направляющие реализацию подходящих средств управления и рассматривающие недопустимые риски информационной безопасности, являются общеизвестными как элементы менеджмента информационной безопасности.

Инструменты и механизмы информационной безопасности включают в себя процессы и процедуры ограничения и разграничения доступа, информационное скрытие; введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); использование методов надежного хранения, преобразования и передачи информации; нормативно административное побуждение и принуждение.

В соответствии с **ГОСТ 27002-2012** «Методы и средства обеспечения безопасности»:

Информационная безопасность организации – это состояние защищенности интересов организации в условиях угроз в информационной сфере.

Защищенность достигается обеспечением совокупности свойств информационной безопасности – конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации.

Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

При этом **цель информационной безопасности (организации)** рассматривается как заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).

Результатом обеспечения ИБ может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Для нормативно-правового обеспечения ИБ организации создается система документов по ИБ.

Система документов по информационной безопасности в организации – это объединенная целевой направленностью упорядоченная совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности.

Товарищи студенты, основополагающим документом по информационной безопасности организации (предприятия) является Концепция информационной безопасности. Рассмотрим содержание данного документа.

Концепция информационной безопасности организации (предприятия) представляет собой документ, в котором определены:

- основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для предприятия;
- основные принципы защиты, определяющие стратегию обеспечения информационной безопасности и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности предприятия;
- модель нарушителя безопасности, определяемую на основе обследования ресурсов системы и способов их использования;
- модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;
- требования безопасности, определяемые по результатам анализа рисков;
- меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований;
- ответственность сотрудников предприятия за соблюдение установленных требований информационной безопасности при эксплуатации информационной системы предприятия.

При этом необходимо учитывать, что риски и эффективность средств управления информационной безопасности меняются в зависимости от складывающихся обстоятельств, поэтому каждая организация обязана выполнять следующие обязанности:

- контролировать и оценивать эффективность имеющихся средств управления и процедур информационной безопасности;
- идентифицировать появляющиеся риски для их рассмотрения;
- выбирать, реализовывать и улучшать должным образом соответствующие меры и средства контроля и управления информационной безопасности.

Товарищи студенты! В соответствии с изученным ранее материалом, системы защиты информации могут рассматриваться по различным уровням, например, система защиты информации государства, отрасли, ведомства, организации или личности. Но система защиты информации для любого уровня определяется «Политикой безопасности информации».

При этом каждая ***организация должна установить свою политику и цели для системы информационной безопасности***. Данная политика необходима, чтобы установить взаимосвязь между всеми элементами системы информационной безопасности и скоординировать все процессы, протекающие в ней, что в свою очередь позволит эффективно достигать цели информационной безопасности организации при использовании системы менеджмента. А т.к. вы

будете специалистами по направлению «Информационная безопасность организации», то далее мы будем рассматривать понятие «Политика безопасности информации (в организации)».

Политика безопасности организации может состоять из принципов безопасности и директив для организации в целом. Она должна отражать более широкий круг аспектов политики организации, включая аспекты, которые касаются прав личности, законодательных требований и стандартов.

Политика информационной безопасности может содержать принципы и директивы, специфичные для защиты конфиденциальной, ценной или иной важной для организации информации. Содержащиеся в ней принципы строятся на основе принципов политики безопасности и, таким образом, согласованы с ними.

При разработке и проведении Политики информационной безопасности в жизнь целесообразно руководствоваться следующими принципами:

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности;
- адекватность (разумная достаточность);
- системность;
- прозрачность для легальных пользователей;
- равностойкость звеньев.

Кратко рассмотрим суть некоторых принципов.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если механизм турникета ломается, турникет должен оставаться в закрытом состоянии, препятствуя проходу людей.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать, программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний

рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен ***принцип простоты и управляемости информационной системы*** в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Принцип адекватности (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемых ресурсов. Вряд ли руководитель потратит деньги на металлическую дверь, суперзамок и сигнализацию, если в помещении нет конфиденциальной информации.

Системность. Конечно, важность этого принципа проявляется при построении крупных систем защиты, но и в небольшой фирме не стоит забывать о важности системного подхода. Он состоит в том, что система защиты должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств.

Прозрачность для легальных пользователей. Можно заставлять пользователей перед каждой операцией для надежной идентификации вводить 10-значный пароль, прикладывать палец к сканеру и произносить кодовую фразу. Но необходимо учитывать, что это будет затруднять доступ пользователей к информации, поэтому необходимо создавать рациональные способы доступа.

Равностойкость звеньев. Звенья – это элементы защиты, преодоление любого из которых означает преодоление всей защиты (например, окно и дверь

в равной степени открывают злоумышленнику путь в защищаемое помещение). Понятно, что нельзя слабость одних звеньев компенсировать усилением других. В любом случае прочность защиты (или ее уровня) определяется прочностью самого слабого звена.

Таким образом, в соответствии с рассматриваемым **ГОСТ 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»:

Политика информационной безопасности организации – формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Правила информационной безопасности включают:

- физическую безопасность объекта. Т.е., охрана территории предприятия должна регулироваться общими правилами. Также доступ на объект рекомендуется контролировать, чтобы избежать риска проникновения злоумышленника;

- безопасность персонала. Сюда относят обеспечение надлежащих условий труда, распределение сотрудников по отделам с конкретными рабочими задачами, в том числе и по информационной безопасности;

- административную и сетевую безопасность – это правила разграничения доступа к данным и практическая реализация алгоритмов защиты локальных сетей предприятия.

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности.

Политики информационной безопасности должны содержать:

- предмет, основные цели и задачи политики безопасности;

- условия применения политики безопасности и возможные ограничения;

- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;

- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;

- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

Данная политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в актуальной, доступной и понятной форме.

В соответствии с ранее рассматриваемым **ГОСТ 27002** «Методы и средства обеспечения безопасности»:

Цель Политики информационной безопасности – обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами, и нормами.

Высшее руководство организации должно установить четкое направление Политики в соответствии с целями бизнеса и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках организации.

Цели Политики информационной безопасности относятся к одной или нескольким из следующих категорий:

- защита ресурсов;
- аутентификация;
- авторизация;
- целостность;
- конфиденциальность;
- аудит безопасности.

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники.

Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

Основными задачами Политики информационной безопасности являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности организации;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности организации;
- организация антивирусной защиты информационных ресурсов организации;
- защита информации организации от несанкционированного доступа и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководителю организации.

Таким образом, мы рассмотрели *предмет, основные цели и задачи политики безопасности*. Далее рассмотрим *условия применения политики безопасности и возможные ограничения*.

Выяснение того, что, от кого и от чего мы будем защищать - большой шаг на пути к ответу на главный вопрос: как защищать?

Итак, следует определить политику применительно к различным элементам защиты:

Политика управления паролями (или, в более общем виде, политика идентификации и аутентификации) может определять периодичность замены паролей, действия, которые необходимо осуществить при компрометации паролей, основные требования к их качеству, процедурам их генерации, распределению основных обязанностей, связанных с генерацией паролей, их сменой и доведением до пользователей, а также основные меры ответственности за нарушение установленных правил и требований. Политика на этом уровне также может устанавливать запрет хранения записанных паролей, запрет сообщать кому-либо свой пароль (в том числе руководителям и администраторам информационных систем) и другие аналогичные ограничения.

Политика установки и обновления версий программного обеспечения не является внутриорганизационной политикой безопасности, но фактически должна либо напрямую использоваться государственными учреждениями и предприятиями, имеющими доступ к информации, составляющей государственную тайну РФ, как политика безопасности, либо ее положения должны быть прямо перенесены во внутренние политики информационной безопасности таких учреждений и предприятий.

Политика приобретения информационных систем и их элементов (программных и аппаратных средств) может включать в себя требования к лицензированию и сертификации используемых программного обеспечения и оборудования, а также определенные требования к фирмам, осуществляющим их поставку и внедрение.

Политика доступа сторонних пользователей (организаций) в информационные системы предприятия может содержать перечень основных ситуаций возможности доступа, критериев и процедур его осуществления, распределение ответственности сотрудников компании.

Политика в отношении разработки программного обеспечения может содержать требования как к вопросам безопасности и надежности программных средств, самостоятельно разрабатываемых предприятием, так и в отношении передачи разработки программных средств сторонним специализированным организациям, а также в отношении приобретения и использования тиражируемых программных библиотек компаний производителей.

Политики использования отдельных универсальных информационных технологий в масштабе всего предприятия могут включать в себя политику использования электронной почты (e-mail); политику использования средств шифрования данных; политику защиты от компьютерных вирусов и других вредоносных программ; политику использования модемов и других аналогичных коммуникационных средств; политику использования Инфраструктуры публичных ключей; политику использования технологии Виртуальных частных сетей (VirtualPrivateNetwork- VPN).

Политика использования электронной почты может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению

конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений.

Политика использования коммуникационных средств может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами. Политика использования мобильных аппаратных средств может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и т.п.).

Политика информационной безопасности может составлять часть документа по общей Политике безопасности организации. Если Политика информационной безопасности распространяется за пределами организации, следует принимать меры в отношении неразглашения конфиденциальной информации.

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики информационной безопасности. Пересмотр Политики информационной безопасности заключается в оценке возможностей по улучшению политики информационной безопасности организации и подхода к менеджменту информационной безопасности в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре Политики информационной безопасности следует учитывать результаты пересмотров методов управления. Для этого должны существовать определенные процедуры пересмотра методов управления, в том числе график или период пересмотра.

Входные данные для пересмотра Политики информационной безопасности должны включать информацию:

- об ответной реакции заинтересованных сторон;
- о результатах независимых пересмотров;
- о состоянии предотвращающих и корректирующих действий;
- о результатах предыдущих пересмотров методов управления;
- о выполнении процесса и соответствии политике информационной безопасности;
- об изменениях, которые могли бы повлиять на подход организации к методам управления информационной безопасностью, включая изменения, касающиеся организационной среды, обстоятельств бизнеса, доступности ресурсов, контрактных, регулирующих и правовых условий или технической среды;
- о тенденциях в отношении угроз и уязвимостей;

- о доведенных до сведения инцидентах информационной безопасности;
- о рекомендациях, данных соответствующими органами.

Выходные данные пересмотра Политики информационной безопасности должны включать любые решения и действия относительно:

- улучшения подхода организации к менеджменту информационной безопасности и ее процессов;
- улучшения мер и средств контроля и управления, и целей их применения;
- улучшения распределения ресурсов и(или) обязанностей.

Пересмотренная Политика должна быть утверждена руководством.

Соответствие Политикам безопасности и стандартам, техническое соответствие.

Цель проведения соответствия: обеспечить уверенность в соответствии систем политикам безопасности организации и стандартам.

Безопасность информационных систем необходимо регулярно пересматривать.

Такие пересмотры необходимо осуществлять по отношению к соответствующим политикам безопасности, а технические платформы и информационные системы должны подвергаться проверке на предмет соответствия применимым стандартам безопасности и документированным мерам, и средствам контроля и управления безопасности.

Руководители должны обеспечить уверенность в том, что все процедуры безопасности в пределах их зоны ответственности выполняются правильно, для того чтобы достичь соответствия политикам и стандартам безопасности.

Руководители должны регулярно анализировать соответствие обработки информации в пределах их зоны ответственности политикам и стандартам безопасности, а также любым другим требованиям безопасности.

Если в результате проведения анализа было ***выявлено какое-либо несоответствие***, руководителям следует:

- определить причины несоответствия;
- оценить необходимость действий с целью обеспечения уверенности в том, что несоответствие не повторится;
- определить и реализовать соответствующее корректирующее действие;
- проанализировать предпринятое корректирующее действие.

Результаты анализа и корректирующих действий, предпринятых руководителями, необходимо регистрировать, и эти записи следует сохранять для аудита информационной безопасности. Руководители должны сообщать результаты лицам, проводящим независимые проверки, если такая независимая проверка имела место в зоне их ответственности.

На этом изложение первого учебного вопроса завершено.

Второй учебный вопрос: «Цель и задачи системы информационной безопасности»

Проблемы информационной безопасности уже более 30 лет находятся в центре внимания специалистов и, можно считать, что за это время были достигнуты следующие результаты:

- проблема информационной безопасности получила всеобщее признание;
- созданы методологические основы информационной безопасности;
- налажено производство средств информационной безопасности;
- организована система подготовки и повышения квалификации специалистов в области информационной безопасности;
- создана государственная система информационной безопасности;
- накоплен богатый опыт практического решения задач защиты информации в системах различного масштаба и назначения.

Приведенное выше, дает основание утверждать, что проблема информационной безопасности имеет определенный базис для дальнейшего целенаправленного развития.

Адекватная защита информационных ресурсов объекта является сегодня обязательным требованием бизнеса. Методы атак на информационные и коммуникационные системы постоянно совершенствуются. С ростом значимости информационных технологий для бизнеса, преступления, связанные с нарушением требований информационной безопасности, все чаще носят направленный характер и совершаются из корыстных побуждений, зачастую, организованными группами лиц.

Товарищи студенты, основой безопасности любой организации является комплексная безопасность.

Комплексная безопасность – система взглядов и практических действий, направленных на создание и поддержание таких условий, которые обеспечивают деятельность всего комплекса мер безопасности, направленных на достижение целей его функционирования.

Система комплексной *безопасности* включает в себя следующие составляющие подсистемы:

- правовую безопасность;
- кадровую безопасность;
- финансовую безопасность;
- инженерно-техническую безопасность;
- экономическую безопасность;
- ***информационную безопасность*;**
- и другие.

Темпы развития информационных технологий и появления новых продуктов и технологий, а также их специфика должны быть учтены средствами и системами защиты IT-ресурсов. Таким образом, усложнение информационных технологий в целом, сопровождается возрастающей степенью зависимости бизнеса от их применения.

В связи с этим, процесс обеспечения информационной безопасности становится непрерывным, а применяемые меры должны носить комплексный характер.

Для решения этих задач в организации (предприятии) создается система информационной безопасности.

Данная система информационной безопасности представляет модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов для достижения деловых целей, основанную на оценке риска и на принятии уровней риска организации, разработанную для эффективного рассмотрения и управления рисками.

Анализ требований для защиты информационных активов и применение соответствующих средств управления, чтобы обеспечить необходимую защиту этих информационных активов, способствует успешной реализации системы информационной безопасности.

Следующие основные **принципы** способствуют созданию **системы информационной безопасности**:

- понимание необходимости создания системы информационной безопасности всеми должностными лицами;
- назначение ответственности за информационную безопасность;
- соединение административных обязанностей и интересов заинтересованных лиц;
- возрастание социальных ценностей;
- оценка риска, определяющая соответствующие меры и средства контроля и управления для достижения допустимых уровней риска;
- безопасность это неотъемлемый, важный элемент информационных сетей и систем;
- активное предупреждение и выявление инцидентов информационной безопасности;
- обеспечение комплексного подхода к менеджменту информационной безопасности;
- непрерывная переоценка и соответствующая модификация системы информационной безопасности.

Роль системы информационной безопасности в организации заключается в совокупности определенных функций и задач обеспечения информационной безопасности организации, устанавливающих допустимое взаимодействие между субъектом и объектом в организации.

К субъектам относятся лица из числа руководителей организации, ее персонал или инициируемые от их имени процессы по выполнению действий над объектами.

Объектами могут быть техническое, программное, программно-техническое средство, информационный ресурс, над которыми выполняются действия.

Товарищи студенты, на предыдущих занятиях было акцентировано ваше внимание на то, что основными документами, определяющим требования к

информационной безопасности для бизнеса являются ГОСТы Р ИСО/МЭК 27001 – 27008.

Требования, предъявляемые **к системе информационной безопасности**, структурированы и сгруппированы по нескольким направлениям.

1. Группа требований, обусловленных характером информации, циркулирующей в информационной системе объекта. К ним относятся:

- степени конфиденциальности информации;
- объемы информации, циркулирующей в информационной системе;
- интенсивность обработки информации.

2. Группа требований, обусловленных архитектурой информационной системы объекта. К ним можно отнести:

- пространственные размеры информационной системы;
- территориальную распределённость информационной системы;
- структурированность компонентов информационной системы.

3. Группа требований, обусловленных условиями функционирования информационной системы объекта. К ним отнесем:

- расположение информационной инфраструктуры системы на территории объекта;
- степень обустроенности информационной инфраструктуры;
- развитость информационных коммуникаций.

4. Группа требований, обусловленных технологией обработки информации в системе. К ним будем относить:

- масштабируемость системы;
- стабильность функционирования;
- доступность технологических решений;
- структурированность технологии обработки информации в системе.

5. Группа требований, обусловленных организацией функционирования информационной системы объекта. К ним можно отнести:

- общую организацию функционирования системы;
- степень и качество укомплектованности кадрами;
- уровень подготовки и мотивации кадров;
- уровень производственной (технологической) дисциплины.

Необходимо отметить, что **ГОСТ Р ИСО/МЭК 27001** «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» определяет:

Система информационной безопасности – это функциональная подсистема системы комплексной безопасности объекта, объединяющая силы, средства и объекты защиты информации, организованные и функционирующие по правилам, установленным правовыми, организационно-распорядительными и нормативными документами по защите информации.

Целью системы информационной безопасности является создание таких условий функционирования информационной системы объекта, при которых обеспечивается выполнение требований по конфиденциальности, доступности и целостности информации, принадлежащей ему.

При этом, **информационная безопасность бизнеса** – это свойство информации сохранять конфиденциальность, целостность и доступность.

В соответствии с целью СИБ, формируются требования к основным характеристикам информации, составляющим сущность ее безопасности в качестве некоторых свойств или условий функционирования информационной системы объекта, определенных **Федеральным законом № 149** «Об информации, информационных технологиях и о защите информации».

В соответствии с требованиями к безопасности информации сформулируем **задачи СИБ**. К таковым можно отнести:

1. Предупреждение появления угроз информационной безопасности.

Реализация этой задачи носит упреждающий характер и должна способствовать такому построению, которое обеспечивает полную невозможность (в идеале) или минимальную возможность появления дестабилизирующих факторов в различных условиях ее функционирования.

2. Обнаружение появившихся угроз и предупреждение их воздействия на информационную систему объекта.

Данная задача решается осуществлением комплекса мероприятий, в результате проведения которых появившиеся угрозы должны быть обнаружены до момента их воздействия на информационную систему и, непосредственно, на информацию, а также должно быть обеспечено недопущение воздействия угроз в условиях их появления и обнаружения.

3. Обнаружение воздействия угроз на информационную систему объекта и локализация этого воздействия.

Решение данной задачи заключается в непрерывном контроле средств, комплексов, систем обработки, хранения и защиты информации с целью своевременного обнаружения фактов воздействия на них угроз.

4. Ликвидация последствий воздействия угроз на информационную систему объекта.

Данная задача решается путем восстановления конфиденциальности, целостности и доступности активов организации, подвергнувшихся угрозам. Анализ причин совершения угроз и принятие мер по недопущению подобных инцидентов информационной безопасности впредь.

Для примера рассмотрим вариант с двумя акустическими закладками – активной (имеющей собственное энергетическое поле) и пассивной (не имеющей собственное энергетическое поле), которые заложены в зале для совещаний.

При выполнении 1 задачи определяются угрозы для зала совещаний и принимаются меры по защите информации. При выполнении 2 задачи обследуется зал и обнаруживается активная закладка. В ходе совещания выполняется 3 задача и, например, обнаруживается пассивная закладка, которая уничтожается или блокируется. При выполнении 4 задачи для обеих закладок проводится разбирательство по факту их установки, и определяются меры по недопущению подобных инцидентов впредь и оценивается ущерб организации.

(**Слайд № 23**). Проведем детальный анализ создаваемой системы информационной безопасности (рис.1).

Рис.1. Укрупненная структура СИБ

Под ***силами системы информационной безопасности*** будем понимать совокупность органов и (или) исполнителей работ, связанных с защитой информации в интересах данного объекта. Следовательно, под силами СИБ подразумевается существование некоторого структурного подразделения, выполняющего задачи управления функционированием данной системы. Характер и масштабы сил СИБ будут зависеть от масштаба объекта, характера и степени конфиденциальности имеющейся информации, а также от объема затрат на выполнение указанных задач. Более детально анализ сил информационной безопасности объекта будет проведен в ходе следующих занятий. Но главным органом системы информационной безопасности является **служба информационной безопасности** организации – организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, направленной на противодействие угрозам информационной безопасности организации.

Средства системы информационной безопасности – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты информационных ресурсов объекта от внутренних и внешних воздействий.

Под ***объектами системы информационной безопасности*** будем понимать *информационные ресурсы,* т.е. любые виды активов информационной системы объекта: структурированная и неструктурированная информация, документы, вычислительная техника, коммуникационное и сетевое оборудование, оргтехника и др., относящиеся к конфиденциальной информации.

Система обеспечения информационной безопасности будет рассмотрена на следующем занятии.

Необходимо отметить, что для успешного внедрения системы информационной безопасности в организации решающими факторами зачастую являются следующие:

- соответствие целей, политик и процедур информационной безопасности целям бизнеса;
- подход и основы для внедрения, поддержки, мониторинга и улучшения информационной безопасности, которые согласуются с корпоративной культурой;
- видимая поддержка и обязательства со стороны руководства всех уровней;
- четкое понимание требований информационной безопасности, оценки рисков и менеджмента рисков;
- эффективный маркетинг информационной безопасности среди всех руководителей, сотрудников и других сторон для достижения осведомленности;
- распространение руководящих указаний политики информационной безопасности и соответствующих стандартов среди всех руководителей, сотрудников и других сторон;
- обеспечение финансирования деятельностей по менеджменту информационной безопасности;
- обеспечение соответствующей осведомленности, обучения и тренинга;
- создание эффективного процесса менеджмента инцидентов информационной безопасности;
- внедрение системы измерений, используемых для оценивания, эффективности менеджмента информационной безопасности и предложений по ее улучшению.

При этом информационная безопасность неразрывно связана с ее нарушениями, и вы также должны понимать значение этого понятия.

Нарушение информационной безопасности организации – это случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

На предыдущих занятиях мы рассматривали компьютерные инциденты. Но кроме этого, существуют **инциденты информационной безопасности** – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность организации.

Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа (ГОСТ Р ИСО/МЭК 27001-2006, пункт 3.6).

На этом изложение второго учебного вопроса завершено.

Третий учебный вопрос: «Применение системного подхода к созданию системы информационной безопасности»

Исходя из основных положений системного анализа, будем рассматривать обозначенную систему информационной безопасности, как функционирование сложной системы в совокупности со всесторонним ее обеспечением.

Оценка соответствия системы информационной безопасности организации установленным требованиям – это деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований информационной безопасности.

Особенностью системного подхода к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы.

Системный подход к созданию системы информационной безопасности базируется на следующих методологических принципах:

• конечной цели - абсолютного приоритета конечной (глобальной) цели;

• единства - совместного рассмотрения системы как целого и как совокупности частей (элементов);

• связности - рассмотрения любой части системы совместно с ее связями с окружением;

• модульного построения - выделения модулей в системе и рассмотрения ее как совокупности модулей;

• иерархии - введения иерархии частей (элементов) и их ранжирования;

• функциональности - совместного рассмотрения структуры и функции с приоритетом функции над структурой;

• развития - учета изменяемости системы, ее способности к развитию, расширению, замене частей, накапливанию информации;

• децентрализации - сочетания в принимаемых решениях и управлении централизации и децентрализации;

• неопределенности - учета неопределенностей и случайностей в системе.

В качестве системного подхода к реализации работ по созданию системы информационной безопасности приведем положения американской концепции системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security), которая строится на 7 этапах реализации.

Первый этап (анализ объекта защиты) состоит в определении того, что нужно защищать и проводится по следующим направлениям:

- какая информация нуждается в защите;

- наиболее важные элементы (критические) защищаемой информации;

- срок жизни критической информации (время, необходимое конкуренту для реализации добытых сведений);

- определяются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;

- классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения управления и т.д.).

Второй этап заключается в выявлении угроз. Он происходит по следующим направлениям:

- определяется, кого может заинтересовать защищаемая информация;

- оцениваются методы, используемые конкурентами для получения этой информации;

- оцениваются вероятные каналы утечки информации;

- разрабатывается система мероприятий по пресечению действий конкурента.

Третий этап заключается в анализе эффективности принятых и постоянно действующих подсистем безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.).

На четвертом этапе проводится определение необходимых мер защиты. На основе проведенных на первых трех этапах аналитических исследований определяются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

Пятый этап включает рассмотрение руководителями фирмы (организации) представленные предложения по всем необходимым мерам безопасности и расчет их стоимости и эффективности.

На шестом этапе осуществляется реализация принятых дополнительных мер безопасности с учетом установленных приоритетов.

На седьмом этапе осуществляется контроль и доведение до персонала фирмы реализуемых мер безопасности.

Более наглядно данный подход отобразить схемой (рис. 2), из которой видно, что данный процесс является циклическим.

Рассматриваемый метод требует серьезной аналитической работы, проводимой аналитической группой по следующим основным направлениям:

- информация о рынке и конкурентном окружении;

- информация о производстве и продукции;

- информация об организационных особенностях предприятия и его финансах.

Известно, что основополагающим принципом создания различных систем безопасности является принцип равно прочности, который предполагает сбалансированность уровней защищенности информационной системы объекта, которые вносят все составляющие системы информационной безопасности организации. Следовательно, говорить о серьезной защите информации в информационной системе объекта возможно только в том случае, когда будет обеспечено комплексное применение всех мер и средств ее защиты.

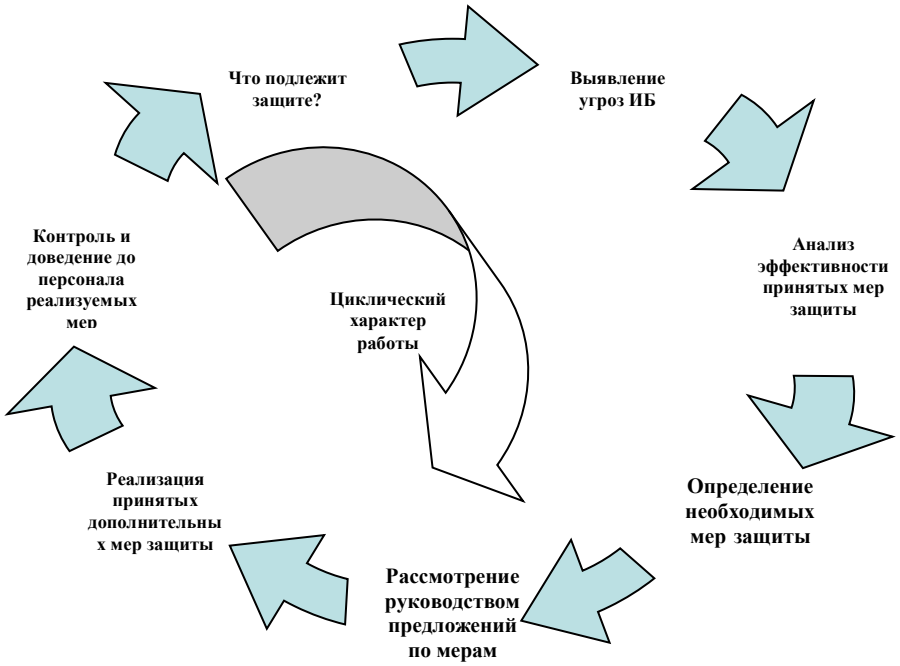

Рис.2. Концепция системного подхода к созданию защиты конфиденциальной информации (OPSEC Operation Security),

На этом изложение второго учебного вопроса завершено.

Литература

1. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

2. ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

3. ГОСТ 27002-2012 «Методы и средства обеспечения безопасности»

4. ГОСТ 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

5. Федеральный закон Российской Федерации №149 от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации».

Заключение

Из представленного учебного материала вам необходимо уяснить понятия «концепции», «политики» и «системы информационной безопасности» и ее содержание.

Доцент кафедры БИТ Д.Власкин