**ЛАБОРАТОРНАЯ РАБОТА №4**

**Цель работы:** изучить аспекты политики безопасности сети на предприятии

**1. Физическая и экологическая безопасность**

Предотвращение неавторизованного доступа к сетевым ресурсам означает, прежде всего, невозможность физического доступа к компонентам сети - рабочим станциям, серверам, сетевым кабелям и устройствам, и т.п. Когда сетевое соединение выходит за пределы вашей зоны влияния, например в точке подключения к внешнему провайдеру интернета, то контроль за физическими аспектами сети теряется - и остается полагаться на другие методы, такие как шифрование и туннелирование. Но оборудование в помещении компании должно находиться под пристальным наблюдением.

**1.1 Безопасные зоны**

**Цель:** предотвратить неразрешенный физический доступ в помещения организации и к ее информации, ущерб и мешающие воздействия для помещений организации и для ее информации.

Средства обработки критической или важной информации должны быть расположены в безопасных зонах, защищенных определенными периметрами безопасности, с подходящими барьерами безопасности и средствами управления доступом. Они должны быть физически защищены от неразрешенного доступа, ущерба и помех.

**Руководство по реализации:**

* Периметры безопасности должны быть четко определены. Периметр безопасности предприятия ограничен пределами здания
* Периметры здания, содержащие средства обработки информации должны быть физически целыми (то есть не должно быть никаких брешей в периметре или зон, где могло бы легко произойти проникновение). Внешние стены имеют твердую конструкцию, а все внешние двери надлежащим образом защищены от неразрешенного доступа при помощи: сигнализации, замков и автоматическими доводчиками; двери и окна должны быть заперты, когда находятся без присмотра, и так же учтена внешняя зашита для окон, особенно на первом этаже (на окнах первого этажа установлены решетки во избежание физического проникновения).
* созданы управляемые персоналом столы регистрации для управления физическим доступом к месту с целью неразрешенного физического доступа, а также при входе расположены турникеты с механизмом пропуска по картам доступа.
* все пожароустойчивые двери в периметре безопасности оснащены сигнализацией, постоянно контролируются и испытываются вместе со стенами для того, чтобы установить необходимый уровень сопротивления в соответствии с подходящими региональными, национальными и международными стандартами;
* в соответствии с национальными, региональными или международными стандартами установлены и регулярно испытываются системы обнаружения вторжения для того, чтобы охватить все внешние двери и доступные окна. В периметре здания офиса расположены камеры наблюдения. Для управления работой камер используется 32-канальные видеорегистраторы. При входе в офис установлены инфракрасные датчики движения под управлением приемно-контрольного прибора охранной сигнализации.
* средства обработки информации, управляемые организацией, физически отделены от средств обработки информации, управляемых третьими сторонами. В здании офиса располагаются серверная и кроссовая комнаты, в которых размещается сетевое оборудование.

**1.2 Средства управления физическим доступом**

**Цель:** Безопасные зоны должны быть защищены подходящими средствами управления доступом для того, чтобы обеспечить доступ только полномочному персоналу.

**Руководство по реализации:**

* дата и время входа и выхода посетителей записываются, все посетители должны находиться под надзором, если их доступ раньше не утверждался, им предоставляется доступ только для конкретных, разрешенных целей; При входе в офис компании будут расположены турникеты для пропуска каждого вошедшего. Сотрудники будут использовать для входа личные карточки, которые дают им доступ в определённые комнаты, в зависимости от специальности. Третьим лицам будут выдаваться временные гостевые карты. Учет посетителей и выдача карт доступа будет производится специальным персоналом. Посетители прежде чем войти должны будут пройти регистрацию. Персонал стола регистрации обязан сообщить посетителям об их правах, полномочиях и проинформировать о правилах использования пропускных карт.
* доступ к зонам, где обрабатывается или хранится важная информация управляется и ограничен только полномочными лицами; доступ к таким зонам имеет только квалифицированный персонал определённого отдела или третьи лица при наличии пропуска с целью ремонта, замены или установки оборудования.
* Средства управления аутентификацией: мастер-карты с уникальным PIN кодом (используется электромеханический замок IronLogic). Контрольный журнал всего доступа содержится в надежном месте;
* от всех служащих, подрядчиков и пользователей третьей стороны и от всех посетителей требуется носить форму видимого идентификационного документа (временные гостевые пропуски для доступа в определённый отдел на определённое время), и они должны немедленно сообщать персоналу службы безопасности, если они сталкиваются с посетителями без сопровождающего и с кем-либо, кто не носит видимого идентификационного документа;
* персоналу вспомогательных служб третьей стороны предоставлен ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется; этот доступ должен быть разрешен и должен постоянно контролироваться;
* права доступа в зоны безопасности регулярно анализируются, обновляются и отменяются при необходимости;
* ключевые средства должны быть расположены так, чтобы избежать доступа к ним широкой публики; все отделы компании, располагаются в отдельных комнатах, защищенных дверьми с доводчиками и электронными замками.
* указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.

**1.3 Защита от внешних и экологических угроз**

**Цель:** обеспечить физическую защиту против ущерба от стихийных бедствий, общественных беспорядков и других форм естественного или искусственного бедствия.

**Руководство по реализации:**

* Внимание должно быть уделено любым угрозам нарушения безопасности, которые представляют соседние помещения, например, огонь в соседнем помещении, протечка воды с крыши или в перекрытиях ниже уровня земли, или взрыв на улице.
* опасные или горючие материалы должны храниться на безопасном расстоянии от безопасной зоны. Несортированная продукция, такая как канцтовары, не должна храниться в безопасной зоне; для этих целей используется специальное помещение
* Резервное оборудование и резервные копии должны быть расположены на безопасном расстоянии для того, чтобы избежать ущерба от бедствия, влияющего на основное местоположение; резервные копии могут располагаться на территории главного офиса, а также в филиале компании
* должно быть предусмотрено и подходящим образом размещено противопожарное оборудование. В периметре здания расположены датчики дыма под управлением контрольно-приемных приборов, ручные пожарные извещатели, огнетушители, а также установлены противопожарные двери. В помещении офиса в определенных местах располагаются планы эвакуации при пожаре. Для ознакомления с правилами пожарной безопасности и действиями на случай возникновения пожара со всеми рабочими и служащими должны проводиться противопожарные инструктажи.

**1.4 Защита оборудования**

**Цель:** предотвратить потерю, ущерб, кражу или раскрытие активов и прерывание в деятельности организации. Оборудование должно быть защищено от физических и экологических угроз.

Защита оборудования (включая, оборудование, используемое вне рабочего места, и вынос имущества), необходима для того, чтобы снизить риск неразрешенного доступа к информации и защититься от потери или ущерба. Защита также должна учитывать размещение и расположение оборудования. Особые средства управления могут потребоваться для защиты от физических угроз, а также для охраны вспомогательных средств, таких как электроснабжение и кабельная инфраструктура.

Оборудование должно быть расположено или защищено так, чтобы снизить риски возникновения экологических угроз и опасностей, а также количество возможностей для неразрешенного доступа.

**1.5 Размещение и обустройство серверного помещения**

**Цель:** обеспечить максимальную защиту серверного помещения, ограничить доступ, обеспечить необходимые условия для работы сетевого оборудования.

**Серверное помещение -** это телекоммуникационное помещение, в котором размещаются распределительные устройства и большое количество активного телекоммуникационного оборудования. В серверном помещении могут размещаться распределительные пункты, пассивные распределительные устройства и активное сетевое оборудование (патч-панели, кроссы, распределительные коробки, коммутаторы, маршрутизаторы)

**Руководство по реализации:**

* Размещение серверного помещения. Серверное помещение следует размещать как можно ближе к магистральным кабельным каналам. Желательно расположить серверное помещение рядом с главным распределительным пунктом.
* Рекомендуемые размеры серверного помещения. Размер серверного помещения выбирается исходя из размера обслуживаемой рабочей области и количества устанавливаемого оборудования. Важно учесть не только размеры самого оборудования, но и способы монтажа, обеспечения доступа и обслуживания оборудования, возможность установки дополнительных устройств. Рекомендуется под серверное помещение использовать помещение без окон.
* Система контроля и управления микроклиматом должна обеспечить в серверном помещении заданный уровень влажности и температуры необходимый для нормального функционирования активного оборудования. Система микроклимата должна обеспечить поддержку температурного режима не только летом, но и зимой и рассчитана на круглосуточную непрерывную работу.
* Серверное помещение должны быть защищено от пыли и вредных веществ, которые могут отрицательно воздействовать на работу оборудования и на материалы оборудования.
* Вибрация отрицательно влияет на работу активного оборудования, контакты и соединения. Необходимо обеспечить освещение в серверном помещении не менее 500 люкс.
* Электропитание освещения серверного помещения и электропитание телекоммуникационного оборудования, установленного в серверном помещении, должно подаваться от разных распределительных электрических щитов. Светильники необходимо размещать на потолке. Требуется использовать для управления освещением одним или несколькими выключателями и располагать их рядом с дверью на высоте 1.5м от уровня пола.
* Подача электропитания в серверное помещение должна осуществляться по выделенному силовому кабелю, желательно напрямую от главного распределительного щита. Требуется установить отдельный электрический распределительный щит для серверного помещения. В аппаратном помещении должна быть установлена магистральная телекоммуникационная заземляющая шина, к которой должны быть подключены заземляющие и соединительные проводники от монтажных конструктивов, телекоммуникационного оборудования, металлических кабелепроводов.
* Необходимо после прокладки кабелей заделать огнеупорным материалом все кабельные вводы в серверное помещение. Потолочные перекрытия, стены и перегородки серверного помещения должны быть несгораемыми и обеспечивать огнестойкость не менее 45 минут. Дверь должна обеспечить огнестойкость не менее 36 минут. Дверь может быть изготовлена из трудно сгораемого материала толщиной не менее 40 мм без внутренних пустот или можно использовать деревянную дверь, но покрыть ее слоем асбеста или обить листовой сталью толщиной не менее 4 мм с двух сторон.

Серверное помещение должна быть оборудована системами:

* охранной сигнализации;
* пожарной сигнализации;
* пожаротушения;
* кондиционирования и вентиляции;
* освещения и аварийного освещения.

**1.7 Защита кабельных соединений**

**Цель:** перехват сетевых данных представляет собой наиболее эффективный метод сетевого хакинга, позволяющий хакеру получить практически всю информацию, циркулирующую по сети. Наибольшее практическое развитие получили средства снифинга, т.е. прослушивания сетей; однако нельзя обойти вниманием и методы перехвата сетевых данных, выполняемые с помощью вмешательства в нормальное функционирование сети с целью перенаправления трафика на хакерский хост, в особенности методы перехвата TCP-соединений. Силовые кабели и кабели дальней связи, по которым передаются данные или вспомогательные информационные услуги должны быть защищены от перехвата или повреждения.

**Руководство по реализации:**

* сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны. Все сетевые кабели располагаются в фальшполу, потолке, что обеспечивает невозможность получения неразрешенного физического доступа к ним.
* силовые кабели должен быть отделены от кабелей дальней связи для того, чтобы предотвратить помехи, так же во избежание влияния помех на сигнал используется кабель U/FTP Cat. 6 с экранированной парой;
* легко различимые маркировки кабелей и оборудования должны использоваться для того, чтобы минимизировать ошибки из-за неправильного обращения, такие как случайная коммутация неправильных сетевых кабелей. Во избежание ошибок при коммутации кабелей необходимо руководствоваться технической документацией СКС и соответствуя таблицам подключений, правильно маркировать кабели;

**1.7 Обслуживание оборудования**

**Цель:** Оборудование должно правильно обслуживаться для обеспечения непрерывной доступности и целостности.

**Руководство по реализации:**

* оборудование должно обслуживаться в соответствии с рекомендуемой поставщиком периодичностью и спецификациями технического обслуживания; должно быть организовано обследование помещений и объектов с целью обнаружения скрыто установленных устройств негласного съема информации
* только полномочный обслуживающий персонал должен выполнять ремонт и обслуживать оборудование;
* должны храниться записи обо всех предполагаемых или фактических дефектах, а также обо всем предупреждающем и корректирующем обслуживании;
* если оборудование включено в график обслуживания, то должны быть реализованы подходящие средства управления, учитывающие, выполняется ли это обслуживание местным персоналом или персоналом, внешним по отношению к организации; если это необходимо, то оборудование должно быть очищено от важной информации, или обслуживающий персонал должен иметь достаточный допуск к конфиденциальной работе;
* все требования, наложенные страховыми полисами, должны быть выполнены.

**1.8 Защита оборудования, находящегося за пределами рабочего места**

**Цель:** Защита должна применяться для оборудования, находящегося за пределами рабочего места, с учетом различных рисков работы за пределами организационных помещений.

**Руководство по реализации:**

* Независимо от собственности, использование любых средств обработки информации за пределами организационных помещений должно быть разрешено руководством.
* оборудование и носители информации, выносимые из помещений, не должны оставляться без присмотра в общедоступных местах; портативные компьютеры при путешествии должны перевозиться в качестве ручной клади и должны быть замаскированы, если возможно;
* все время должны соблюдаться инструкции изготовителя для защиты оборудования, например, защита от сильных электромагнитных полей;
* средства управления домашней работой должны быть определены оценкой риска, и подходящие средства управления должны быть применены, по остановке, например, запирающийся картотечный блок, политика чистого стола, средства управления доступом для компьютеров и безопасная связь с офисом.
* для защиты оборудования, находящегося за пределами рабочего места, должен быть принят адекватный объем страховой ответственности.
* Риски нарушения системы безопасности, например, риск ущерба, кражи или подслушивания, могут значительно различаться в зависимости от местоположения и должны быть учтены при определении наиболее подходящих средств управления.
* Оборудование, используемое для хранения и обработки информации, включает все формы персональных компьютеров, органайзеров, мобильных телефонов, смарт-карт, бумаг или другую форму, которая держится для домашней работы или уносится с места обычной работы.

**1.9 Безопасная ликвидация или повторное использование оборудования**

**Цель:** Все элементы оборудования, содержащие носители информации, должны быть проверены для обеспечения того, что любые важные данные и лицензионное программное обеспечение были удалены или надежно затерты перед ликвидацией.

**Руководство по реализации:**

* Устройства, содержащие конфиденциальную информацию, должны быть физически уничтожены, или информация должна быть уничтожена, удалена или затерта, используя соответствующие методы с целью сделать оригинальную информацию невосстановимой, вместо того, чтобы использовать стандартную функцию удаления или форматирования.
* Поврежденные устройства, содержащие важные данные, могут потребовать оценки рисков для того, чтобы определить, должны ли элементы быть уничтожены физически, отправлены для ремонта или забракованы.

**1.10 Вынос имущества**

**Цель:** Оборудование, информация или программное обеспечение не должны выноситься за пределы рабочего места без предварительного разрешения.

**Руководство по реализации:**

* служащие, подрядчики и пользователи третьей стороны, которые имеют полномочие разрешать вынос активов за пределы рабочего места, должны быть четко определены;
* должны быть установлены ограничения на время выноса оборудования, и возвраты должны быть проверены на соответствие;
* если это необходимо и уместно, то оборудование должно быть записано как вынесенное с рабочего места и записано по возвращении, эти операции должны выполнятся на пропускном пункте при входе.
* Внезапные проверки, предпринимаемые с целью обнаружить неразрешенный вынос имущества, также могут проводиться для того, чтобы обнаружить неразрешенные записывающие устройства, оружие и т.п., и предотвратить их внос на рабочее место. Такие внезапные проверки должны выполняться согласно соответствующим законам и нормам. Люди должны быть осведомлены о том, проводятся ли внезапные проверки, и проверки должны выполняться только с разрешением, соответствующим требованиям закона и юридическим требованиям.

**1.11 Непрерывность бизнес-процессов**

**Цель:** cобытия, которые могут вызвать прерывания деловых процессов, должны быть определены, вместе с вероятностью и влиянием таких прерываний и их последствий для защиты информации.

Аспекты обеспечения непрерывности бизнеса, связанные с защитой информации, должны быть основаны на выявлении событий (или последовательности событий), которые могут вызвать прерывания в деловых процессах организаций, например, сбой оборудования, человеческие ошибки, кражи, пожар, стихийные бедствия и акты терроризма. За оценкой рисков должно последовать определение вероятности и влияния таких прерываний с точки зрения времени, масштаба ущерба и периода восстановления.

Именно IT-системы и сервисы, обеспечивающие поддержку критически важных бизнес-процессов, оказываются наиболее чувствительными к воздействиям стихийных бедствий, аварий и катастроф.

**Руководство по реализации:**

Для обеспечения защиты информации и непрерывности основных процессов в компании следует придерживаться следующих правил:

* Конфиденциальность - обеспечение доступности информации только для тех кто имеет соответствующие полномочия
* Доступность - обеспечение доступа к информации авторизованным пользователям в нужный момент времени
* Целостность - обеспечение точности и полноты информации, а так же методов её обработки

Как и большинство планов компании, план непрерывности бизнеса должен развиваться и совершенствоваться в течение жизненного цикла каждого бизнес-процесса по мере накопления информации о деятельности организации и сопряженных рисках, должен охватывать все основные функции компании и содержать документально оформленные и практически проверенные процедуры, следование которым обеспечит непрерывность основных бизнес-процессов или минимизацию времени их перерыва.

Сроки и качество внедрения систем непрерывности бизнеса и систем управления информационной безопасностью напрямую зависят от квалификации персонала. Невозможно обеспечить протекание бизнес-процессов без простоев, большую роль в этом играет человеческий фактор и уровень квалификации и подготовленности сотрудников компании.

Одним из основных аспектов обеспечения непрерывности процессов на предприятии является физическая безопасность информации и оборудования, а так же возможность восстановления информации в кратчайшее время при сбоях в системе.

1) Компьютерная система энергоемка, и потому первое условие ее функционирования - бесперебойная подача электроэнергии. Необходимой частью информационной системы становятся источники бесперебойного питания для серверов, а по возможности, и для всех локальных рабочих станций. В данной компании предполагается использование источников бесперебойного питания Mustek PowerMust 848 Offline (98-UPS-VN008) - для рабочих станций и ИБП APC Smart-UPS RM 3000VA 2U LCD (SMT3000RMI2U) - для серверов и сетевого оборудования, что обеспечит возможность автономной работы данного оборудования на время, достаточное для корректного завершения работы ОС, сохранения данных, завершения работы приложений и корректного выключения.

2) Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных. Резервное копирование будет производиться с определённой периодичностью, в зависимости от количества и объёма поступления важных и конфиденциальных данных. Резервные копии планируется хранить на сетевом накопителе NAS Synology RackStation RS810RP+, который предоставляет максимальный объём данных 12 Тб. При увеличении объёма резервируемой информации возможно приобретение дополнительных СХД. Для управления процессами резервирования предполагается использование корпоративного решения Handy Backup Server, которое позволит централизовано выполнять резервное копирование и восстановление данных, хранимых на серверах и клиентских компьютерах.

3) Так же на случай сбоев в сети и невозможности прямого доступа персонала к общим файлам по каким либо причинам предусматривается использование автономных файлов, что позволит не прерывать работу с данными и корректно сохранить их до восстановления связи в сети.

4) На предприятии должен иметься специальный документ: «План обеспечения непрерывной работы и восстановления», в котором будут описываться следующие положения:

* классификация возможных (значимых) кризисных ситуаций и указание источников получения информации о возникновении кризисной ситуации;
* перечень основных мер и средств обеспечения непрерывности процесса функционирования ИС и своевременности восстановления ее работоспособности;
* общие требования к подсистеме обеспечения непрерывной работы и восстановления;
* типовые формы для планирования резервирования ресурсов подсистем ИС и определения конкретных мер и средств обеспечения работы и восстановления;
* порядок действий и обязанности персонала по обеспечению непрерывной работы и восстановлению работоспособности системы.

Все сотрудники компании в обязательном порядке должны быть ознакомлены с данным документом.

**2.** **Информационная безопасность**

**Цель:** безопасность информации предполагает отсутствие недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на ресурсы, используемые в автоматизированной системе. Критериями информационной безопасности являются конфиденциальность, целостность и будущая доступность информации. Система защиты информации на предприятии преследует такие цели как предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP. Сетевые атаки через Интернет могут быть классифицированы следующим образом:

**Сниффер пакетов** (sniffer - в данном случае в смысле фильтрация) - прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).

**IP-спуфинг** (spoof - обман, мистификация) - происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.

Отказ в обслуживании (Denial of Service - DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

**Парольные атаки** - попытка подбора пароля легального пользователя для входа в сеть.

**Атаки типа Man-in-the-Middle** - непосредственный доступ к пакетам, передаваемым по сети.

**Сетевая разведка** - сбор информации о сети с помощью общедоступных данных и приложений.

**Несанкционированный доступ** (НСД), который не может считаться отдельным типом атаки, так как большинство сетевых атак проводятся ради получения несанкционированного доступа.

Защита информации в сети может быть улучшена за счет использования специальных программных средств, включающих программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки - ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

**2.1 Защита информации на уровне сети**

* Подключение ко всем сетевым устройствам по безопасному протоколу SSH версии 2, обеспечивающего защищенную аутентификацию, соединение и безопасную передачу данных между хостами сети, путем шифрования, проходящего через него трафика, с возможной сжатия данных.
* Аутентификация на сетевом оборудовании CISCO производится через удаленный сервер с помощью протокола Tacacs+, что исключает вероятность подключения к устройствам не доверенных лиц.
* Использование механизма PortFast на коммутаторах уровня Access который позволяет порту пропустить состояния listening и learning и сразу же перейти в состояние forwarding. Это применяется для того чтобы включать рабочие станции и сервера в сеть немедленно, без ожидания конвергенции Spanning Tree
* Использование механизма BPDU Guard на всех портах коммутаторов уровня Access, этот механизм отключает порт коммутатора если на нём включен Port Fast и на этот порт приходят STP сообщения.
* Запрещение передачи информации между VLAN с использованием списков доступа
* Использование технологии PAT(NAT Overload). Это позволяет многим приватным IP адресам использовать один внешний адрес для выхода во внешнюю сеть.
* Использование файрвола с учетом состояния CBAC на маршрутизаторах. Это возможность, заложенная в Cisco IOS, позволяющая определять, какой трафик должен быть разрешен на основании списков доступа (access list). Списки доступа CBAC включают инструкции анализа ip, позволяющие удостовериться в отсутствии нападения прежде, чем трафик будет передан внутрь локальной сети. CBAC может использоваться совместно с NAT, в этом случае списки доступа должны ссылаться на внешние адреса, а не на адреса локальной сети.
* Выдача IP адресов по DHCP в привязке к VLAN.
* Использования протокола VPN для подключения к сети провайдера и сети филиала, что обеспечивает высокую защиту передаваемой информации за счёт специальных алгоритмов шифрования и надёжных механизмов аутентификации. Используются протоколы: L2TP - для подключения к филиалу, SSTP - для удаленных пользователей.
* Для журналирования событий сетевого оборудования cisco на удаленном сервере используется syslog. Такой подход позволяет централизовать сбор важных лог сообщений что в свою очередь упростить их поиск и разбор, это позволит иметь полную статистику происходящих с оборудованием событий, проводить анализ и заранее выявлять возможные проблемы.

**2.2 Защита информации на пользовательском уровне**

* На клиентских компьютерах и серверах предполагается установка антивирусной программы ESET NOD32 Bussines Edition Antivirus, что обеспечит централизованную защиту файловых серверов и рабочих станций от троянских и шпионских программ, червей, рекламного ПО, фишинг-атак и других интернет-угроз в организации. Решение включает в себя приложение ESET Remote Administrator (ERA), которое обеспечивает централизованное администрирование антивирусного решения. С помощью решения ESET Remote Administrator можно удаленно осуществлять инсталляцию и деинсталляцию программных продуктов ESET, контролировать работу антивирусного ПО, создавать внутри сети серверы для локального обновления продуктов ESET («зеркала»), позволяющие существенно сокращать внешний интернет-трафик.
* Брандмауэр Windows обеспечит препятствие несанкционированному доступу вредоносных программ из Интернета и локальной сети.
* Групповые политики
* Использование технологий NPS и NAP для проверки клиентских компьютеров и удалённых пользователей на соответствие их конфигурации и состояния требованиям политики безопасности.
* Установка операционных систем и программ будет проводиться централизовано через сервер WDS, что значительно облегчает задачу внедрения операционных систем. Установка обновлений операционных систем и ПО планируется осуществлять так же через отдельный сервер с помощью программы WSUS. Эта служба позволяет скачивать актуальные обновления с сайта Microsoft, которые могут быть распространены внутри корпоративной локальной сети. Это экономит внешний трафик компании и позволяет быстрее устанавливать исправления ошибок и уязвимостей в операционных системах Windows на рабочих местах, а также позволяет централизованно управлять обновлениями серверов и рабочих станций.
* Использование локального центра сертификации на уровне домена.
* Автоматическая выдача сертификатов безопасности (защищенная почта, проверка подлинности клиентов, серверов).
* Агент восстановления EFS. Агент восстановления закрытых ключей. Агентом восстановления является пользователь, уполномоченный расшифровывать данные, зашифрованные другим пользователем, если пользователь утратил закрытые ключи сертификата шифрования или учетная запись пользователя удалена и требуется восстановить зашифрованные данные. Шифрование EFS будет использоваться на специализированном сервере хранения конфиденциальных данных.
* Для шифрования информации на локальных дисках и клиентских мобильных компьютерах (и съёмных дисках) используется BitLocker. Этот сервис позволяет защитить все данные, от документов до паролей, путем шифрования всего диска, на котором хранятся системные файлы Windows и данные пользователей. Когда BitLocker работает, любой сохраняемый на жестком диске файл будет автоматически зашифрован.
* Использование службы RMS для защиты пользовательских документов. AD RMS обеспечит конфиденциальности документов пользователей независимо от способа хранения и распространения. Документы, защищенные AD RMS, шифруются, а автор может устанавливать разрешения для тех, кто получит доступ к данным.
* Возможность работы пользователей с автономными файлами. С помощью этого механизма пользователи смогут открывать и корректировать файлы, находящиеся в общих папках, даже отключившись от сети по каким либо причинам. При отключении от сети автономные файлы извещают об этом пользователя. При автономной работе, не имея соединения с сетью, пользователь не теряет способности просматривать сетевые устройства и работать со своими файлами. Права доступа в автономном режиме работы остаются такими же, какие они были при наличии соединения с сетью.
* Следует ознакомиться с фоновыми процессами, выполняемыми на всех серверах сети, и отключить лишние.
* При соблюдении всех правил конфигурирования программного обеспечения и проведения административных мероприятий вероятность несанкционированного доступа к информации значительно снижается.

**3. Человеческий фактор**

**Цель:** пользователям компьютеров следует руководствоваться перечисленными ниже мерами предосторожности в отношении всех компьютерных и телекоммуникационных ресурсов и служб. Компьютерные и телекоммуникационные ресурсы и службы включают в себя (но не ограничиваются) следующее: компьютеры, серверы файлов, рабочие станции, автономные компьютеры, мобильные компьютеры, программное обеспечение, а также внутренние и внешние сети связи (интернет, коммерческие интерактивные службы и системы электронной почты), к которым прямо или косвенно обращаются компьютерные устройства Компании.

**Руководство по реализации:**

* Пользователи должны соблюдать условия всех программных лицензий, авторское право и законы, касающиеся интеллектуальной собственности.
* Неверные, навязчивые, непристойные, клеветнические, оскорбительные, угрожающие или противозаконные материалы запрещается пересылать по электронной почте или с помощью других средств электронной связи, а также отображать и хранить их на компьютерах компании. Пользователи, заметившие или получившие подобные материалы, должны сразу сообщить об этом инциденте своему руководителю.
* Все, что создано на компьютере, в том числе сообщения электронной почты и другие электронные документы, может быть проанализировано руководством компании.
* Пользователям не разрешается устанавливать на компьютерах и в сети компании программное обеспечение без разрешения системного администратора.
* Пользователи не должны пересылать электронную почту другим лицам и организациям без разрешения отправителя.
* Пользователям запрещается изменять и копировать файлы, принадлежащие другим пользователям, без разрешения владельцев файлов.
* Запрещается использование без предварительного письменного разрешения компьютерных и телекоммуникационных ресурсов и служб компании для передачи или хранения коммерческих либо личных объявлений, ходатайств, рекламных материалов, а также разрушительных программ (вирусов и/или самовоспроизводящегося кода), политических материалов и любой другой информации, на работу с которой у пользователя нет полномочий.
* Пользователь несет ответственность за сохранность своих паролей для входа в систему. Запрещается распечатывать, хранить в сети или передавать другим лицам индивидуальные пароли. Пользователи несут ответственность за все транзакции, которые кто-либо совершит с помощью их пароля.
* Возможность входа в другие компьютерные системы через сеть не дает пользователям права на подключение к этим системам и на использование их без специального разрешения операторов этих систем.
* Весь персонал компании должен в обязательном порядке быть ознакомлен с вышеперечисленными правилами во избежание нарушений. Для реализации этого на предприятии должен иметься документ «Памятка пользователю», в котором будут описаны общие обязанности сотрудников подразделений при работе со средствами информационной системы и ответственность за нарушение установленных порядков.

**4. Аудит и контроль изменений конфигурации систем**

**Цель:** обеспечить проведения аудита и контроля информационной системы в целях оценки её текущего состояния и уровня соответствия бизнес процессам компании. Аудит комплексной безопасности бизнеса в первую очередь направлен именно на выявление имеющихся и предупреждение возможных негативных для предприятия факторов, а также на алгоритм создания и поддержания комфортных условий для занятия бизнесом. Под комфортом в данном случае подразумевается создание наиболее эффективной, экономически выгодной, актуальной и конкурентоспособной системы, которая позволила бы свести к минимуму предпринимательские риски клиентов.

**Руководство по реализации:**

Используемые в работе IT технологии имеют огромное влияние на производительность труда сотрудников и компании в целом, они могут менять её как в положительном так в отрицательном направлении. Любая информационная система должна строго соответствовать предъявляемым к ней требованиям, иначе она помимо своей неэффективности снижает общую эффективность бизнеса.

Для аудита и контроля изменений конфигурации систем в данной компании предполагается использовать продукт для управления IT-инфраструктурой на основе Microsoft Windows и смежных устройств System Center Configuration Manager (SCCM).

**Функциональность SCCM можно разделить на три больших класса:**

**Инвентаризация и отчеты**

* Инвентаризация аппаратного обеспечения (Hardware inventarization)
* Инвентаризация программного обеспечения (Software inventarization)
* Слежение за используемым ПО и лицензиями (Asset Intelligence)
* Отчеты (Reporting)

**Развертывание приложений и ОС:**

* Развертывание операционных систем (OS Deploy)
* Распространение ПО (Software distribution)
* Распространение и управление виртуализированным ПО (Application virtualization management)
* Управление обновлениями (Software update)

**Управление клиентскими устройствами**

* Мониторинг используемых программ (Software metering)
* Удаленное управление клиентами (Remote management)
* Управление мобильными устройства (Modile device management)
* Поддержка заданной конфигурации (Desied configuration manager)
* Защита подключающихся к сети (Network access protection)