Программный комплекс
«РЕДШЛЮЗ»

Поддержка жизненного цикла

Версия 1.0

МОСКВА
2017

Содержание

Введение

В данном документе изложены меры безопасности разработки, применяемые в ООО «Ред Софт». Они охватывают физические, процедурные, относящиеся к персоналу и другие меры безопасности, используемые применительно к среде разработки. Он также содержит требования к физической безопасности местоположения разработки и к контролю за отбором и наймом персонала разработчиков.

1 Меры физической безопасности

Физическая охрана — комплекс мер, направленных на обеспечение безопасности функционирования объекта, сохранности его материального имущества, защиту жизни и здоровья его персонала.

В ООО «Ред Софт» физическая охрана объекта осуществляется при помощи непосредственного присутствия сотрудников охраны на охраняемой территории. Задачи физической охраны:

- контроль пропускного режима;
- досмотр автотранспорта;
- предотвращение краж;
- обход объекта и прилегающей территории;
- мониторинг системы видеонаблюдения;
- слежение за посетителями, сотрудниками предприятия;
- охрана материальных ценностей, находящихся в свободном доступе;
- принятие первичных мер по устранению технических аварий и возгораний;
- предотвращение несанкционированного доступа;
- повышение и поддержание высокого статуса объекта/предприятия;
- предупреждение проникновения на территорию предприятия, в служебные помещения и охраняемые зоны посторонних лиц;
- обеспечение порядка вноса (выноса), ввоза (вывоза) материальных ценностей и входа (выхода) сотрудников и клиентов;
- обеспечение физической безопасности персонала.

Все помещения предприятия, требующие повышенного уровня безопасности, находятся в наиболее охраняемых и наблюдаемых зонах. Что создает злоумышленнику наибольшую проблему при проникновении в охраняемую зону и при осуществлении противоправных действий.

Физическая защита серверов строится на оборудовании специальных серверных помещений, с повышенными требованиями к пожарной безопасности, вентиляции, с постоянной температурой и влажностью воздуха.

Для предотвращения возможных нарушений безопасности по вине человека (например, отключение сервера в случае ошибки работника или незаконного проникновения в серверное помещение) предусмотрен комплекс организационных мер – усиленная охрана серверных помещений, ограничение доступа лиц, имеющих право находится там.

Всё оборудование в серверной размещено в закрытых шкафах или на открытых стойках, число которых определяется исходя из имеющегося оборудования, его типоразмеров и способов монтажа. Для обеспечения необходимого температурного режима, применяются дополнительные вентиляторы, встраиваемые системы охлаждения и модули отвода горячего воздуха.

Коммуникационные кабели в серверной проводятся в лотках, проложенных в нишах фальшпола или фальшпотолка. Вводные каналы в телекоммуникационные шкафы и стойки должны обеспечивать свободную протяжку требуемого количества кабелей вместе с оконечными разъемами.

Коммутация активного сетевого оборудования с рабочими местами

осуществляется с помощью патч-панелей, при этом все они, как и кабели, должны иметь маркировку для однозначной идентификации каждого кабеля.

Серверное помещение оборудовано источниками бесперебойного питания, позволяющими либо отключить сервер не аварийно, а предварительно сохранив всю информацию, либо поддержать систему в рабочем состоянии до подключения резервных источников питания.

В здании организована подсистема распределения электропитания, в которую входят распределительные щиты и кабели питания, ведущие как к оборудованию, так и к рабочим местам пользователей. Для того, чтобы при проведение ремонтных, профилактических и других работ не пришлось отключать общую систему электропитания, всех её потребители разделены на группы, причём, каждая группа имеет свой автомат защиты сети.

В серверной предусмотрена подсистема технологического заземления, отдельная от защитного заземления здания. Её подсоединение к заземлению здания производится непосредственно у защитных электродов, расположенных в грунте. Заземлению должны подвергаться все металлические элементы и конструкции серверной, каждый шкаф или стойка заземляются отдельным проводником.

Для продолжения работы в случае полной потери внешнего электроснабжения в серверной предусмотрено аварийное освещение, питание которого осуществляется автономно от системы общего электропитания помещения.

Система контроля доступа предотвращает попадание в серверную посторонних: лиц, в чьи обязанности не входят монтаж, эксплуатация и техническое обслуживание оборудования. Блокирование помещения осуществляется с помощью различных типов замков.

Система видеонаблюдения служит для визуального контроля обстановки в серверной. Применением видеокамер с разрешением, позволяющим уверенно различать лица сотрудников, позволяет однозначно идентифицировать возможного нарушителя.

Система охранной сигнализации выполняется отдельно от систем безопасности всего здания и имеет собственный источник резервного питания. Сигналы оповещения поступают на специально предусмотренный для этого пульт в помещении круглосуточной охраны.

Подсистема пожарной сигнализации (ППС) обеспечивает в помещениях контроль за температурной и наличием дыма. Сигналы оповещения ППС выводятся на отдельный пульт в помещении круглосуточной охраны. Во всех помещениях имеются средства пожаротушения.

2 Процедурные меры безопасности

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности.

2.1 Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше - с составления описания должности. Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее проверяется кандидат: наводятся о них справки, проводятся беседы с бывшими сослуживцами, внимательно изучается резюме кандидата, проверяются, указанные в нем данные и т.д.

Когда кандидат определен, он, проходит стажировку (испытательный срок) в организации, во время которой он подробно знакомится со служебными обязанностями, а также с нормами и процедурами информационной безопасности организации. Это позволяет убедиться, чтобы меры безопасности были им усвоены до вступления в должность и до получения им доступа к каким-либо конфиденциальным данным.

При заключении трудового договора каждый работник также подписывает Соглашение о неразглашении сведений конфиденциального характера, в которых он обязуется:

- во время работы в Организации не раскрывать сведения конфиденциального характера ООО «Ред Софт», третьим лицам (за исключением случаев привлечения последних к деятельности, требующей раскрытия такой информации и только в том объеме, в котором необходимо для реализации целей и задач Организации, с письменного разрешения руководства Организации);
- не использовать ставшие ему известными или разработанные им сведения конфиденциального характера, иначе, как в интересах Организации;
- соблюдать указанные в Положении о защите конфиденциальной информации ООО «Ред Софт» требования и правила обращения со сведениями конфиденциального характера;
- в случае прекращения работы в Организации, сразу же возвратить Организации все документы и другие материалы, содержание которых содержит сведения конфиденциального характера, полученные в ходе выполнения Работником своих служебных обязанностей;
- в течение 3-х (трех) лет после увольнения не раскрывать (не передавать) третьим лицам сведений конфиденциального характера Организации.

С этого момента ведется контроль за действиями сотрудника: логируются его действия, которые могут нарушить политику безопасности организации, регистрируются изменения в его обязанностях и правах на доступ к определенной информации.

В случае увольнения сотрудника все его учетные записи блокируются и закрывается доступ ко всем информационным ресурсам. Так же сдаются криптографические ключи, если они им использовались.

2.2 Поддержание работоспособности

В процессе поддержания работоспособности информационных систем может создаться угроза безопасности организации. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Можно выделить следующие направления повседневной деятельности ООО «Ред Софт»:

- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Поддержка программного обеспечения - одно из важнейших средств обеспечения целостности информации. На критически важных компьютерах и серверах организации отслеживается актуальность установленных антивирусных продуктов, и программ, которые могут повлиять на безопасность компьютера или разрабатываемого программного продукта. При необходимости уполномоченный администратор может провести контроль за отсутствием неавторизованного изменения программ и прав доступа к ним.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. В случае неудачного обновления программного компонента имеется возможность возврата к прошлой, работающей, версии.

Резервное копирование необходимо для восстановления программ и данных после аварий. Резервные копии создаются по расписанию или по запросу уполномоченного администратора и один из экземпляров резервных копий размещается в месте, отличном от обычного резервного хранения (сервер, физически размещенный в другом подразделении, или иное). Периодически проверяется возможность восстановления информации с копий.

Управление носителями информации с конфиденциальной информацией подразумевает их учет, регистрацию, и отслеживание доступа. А также процедуры их уничтожения.

Документирование - неотъемлемая часть информационной безопасности. Вся документация поддерживается в актуальном состоянии и отражает текущее состояние дел. Доступ к документации зависит от уровня конфиденциальности документа и разрешений на это у работника.

Регламентные работы - серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и поэтому доступ к выполнению подобных работ в организации имеют

только те работники, которые имеют необходимую квалификацию и необходимый уровень доверия.

Правила безопасности, принятые в компании, предусматривать набор действий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Сотрудник, обнаруживший нарушение информационной безопасности должен немедленно сообщить о факте нарушения непосредственному руководителю. Далее в зависимости от опасности выявленного факта принимается решение о мерах по устранению нарушения.

2.3 Реакция на нарушения режима безопасности

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

При выявлении факта нарушения режима безопасности руководитель организации или отдела максимально оперативно пытается установить источник нарушения и нарушителя, локализовать возникший инцидент и постараться принять необходимые меры для уменьшения вреда, который может нанести безопасности в целом или конкретному объекту.

Для предупреждения повторных нарушений в будущем, после выявления всех обстоятельств нарушения, производится разбор с привлечением всех причастных лиц и принимаются необходимые организационно-административные меры.

3 Технические меры безопасности

В рамках технических мер безопасности ООО «Ред Софт» использует следующие:

3.1 Аутентификация пользователей

Каждый пользователь выполняет процедуры входа в компьютер, используя свой логин и пароль как средство для идентификации в начале работы. Каждый пользователь инструктируется о необходимости создания пароля определенной сложности и периодической его смене.

3.2 Процедуры авторизации

Для получения доступа к ресурсам, размещенным вне компьютера пользователя работник должен пройти авторизацию и подтвердить свои полномочия на работу с тем или иным ресурсом. Права и разрешения на работу с ресурсами определяются ответственным администратором по согласованию с непосредственным руководителем работника.

Ответственный за информационную безопасность знает, кто имеет право доступа в помещения с серверным оборудованием и должен контролировать отсутствие посторонних.

3.3 Предосторожности при работе

При нормальном функционировании организации:

- отключаются неиспользуемые терминалы;
- закрываются комнаты, где находятся терминалы;
- разворачиваются экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются;
- выключаются компьютеры в нерабочие часы.

3.4 Разработка программного обеспечения

Вся разработка программного обеспечения в «Ред Софт» ведется с использованием свободных сред разработки, таких как: NetBeans, Eclipse и других. Для управления версиями используется система управления версиями Subversion (также известная как «SVN») — свободная централизованная система управления версиями. Сборка программных продуктов производится на специально выделенных для этого виртуальных серверах, доступ к которым имеет ограниченное число лиц, уполномоченных для работы с ними.

3.5 Физическая безопасность

В защищаемых компьютерных системах необходимо принимать меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Пожарная сигнализация и системы пожаротушения регулярно проверяются.

Температура во всех помещениях контролируется кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. В помещениях запрещено курить, принимать пищу и пить возле ПЭВМ. Компьютеры должны

размещаться как можно дальше источников большого количества воды, например трубопроводов.

3.6 Дублирование офисов

В случае возникновения внештатных ситуаций, когда становится невозможным работа одного из офисов компании, часть сотрудников и выполняемой работы может быть перенесена в дублирующий офис. Таким образом, организуется возможность продолжения работы над критически важными элементами систем.

3.7 Резервирование каналов связи

При отсутствии связи с внешним миром и своими подразделениями, офис оказывается парализованным, потому большое значение имеет резервирование внешних и внутренних каналов связи. При аварийных ситуациях в офисах организации имеется запасной канал передачи данных, который обеспечит бесперебойную работу офиса до восстановления основного канала.