соответствует оригиналу

УТВЕРЖДАЮ
Заместитель главы администрации
Чернянского района –
руководителя аппарата
Г.Г. Федоров _____

«26» апреля 2013 г.

Политика информационной безопасности
корпоративной локально-вычислительной сети администрации муниципального района «Чернянский район» Белгородской области

Информация является ценным и жизненно важным ресурсом администрации муниципального района «Чернянский район» (далее – Учреждение). Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты конфиденциальных сведений от случайного и преднамеренного изменения, копирования и уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Учреждении.

Защита конфиденциальных сведений и обеспечение безопасности всех информационных ресурсов является одной из первоочередных задач Учреждения. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной ресурс Учреждения.

Данная политика регламентирует порядок организации с целью обеспечения сохранности и безопасности информации, как в самом Учреждении, так и при осуществлении деятельности утвержденной уставом.

Предметом указной Политики являются:

- порядок доступа к конфиденциальной информации;
- защита информационных систем от несанкционированного доступа;

– защита внутренних ресурсов сети от вмешательства извне;

– доступ и регистрация в автоматизированной системе;

– управление доступом к телекоммуникационному оборудованию, кабельной инфраструктуре здания, серверным помещениям;

– разграничение прав доступа на разделяемые сетевые ресурсы;

– использование ресурсов глобальных информационных систем, включая Интернет;

– защита серверов и рабочих станций пользователей локальной сети от внешних и внутренних атак, вирусов, атак типа «отказ в обслуживании» и других разновидностей информационных угроз;

– дублирование, резервирование и раздельное хранение конфиденциальной информации;

– обеспечение бесперебойного функционирования информационных систем Учреждения.

Правовую основу настоящей Политики составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

1.1 Цели и задачи настоящей Политики

Данная Политика предусматривает выполнение и реализацию комплекса руководящих принципов, правил, процедур и практических приёмов в области защиты информации, которые регулируют управление, защиту и распределение конфиденциальной информации, а так же защиту информации Учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Основными целями настоящей Политики являются:

– сохранение конфиденциальности критичных информационных ресурсов;

– обеспечение непрерывности доступа к информационным ресурсам для поддержки деятельности Учреждения;

– защита целостности информации с целью поддержания возможности Учреждения по принятию эффективных управленческих решений;

– повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;

– определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности Учреждения.

Общее руководство обеспечением информационной безопасности осуществляет руководитель Учреждения.

1.2 Область применения настоящей Политики

Учреждение осуществляет защиту конфиденциальной информации и ресурсов информационной системы, введенной в эксплуатацию в целях осуществления ею деятельности предусмотренной Уставом.

Настоящая Политика распространяется на все структурные подразделения Учреждения, а так же на информацию и информационные ресурсы Учреждения, и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах.

Соблюдение настоящей Политики обязательно для всех сотрудников Учреждения (как постоянных, так и временных).

В договорах с третьими лицами, получающими доступ к защищаемой информации Учреждения, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

1.3 Анализ компьютерной сети

Компьютерная сеть представляет собой комплекс программных и аппаратных средств. Под аппаратными средствами подразумевается следующее оборудование:

– серверное (предназначенное для хранения и обработки больших массивов информации),

– оборудование технической защиты (криптомаршрутизаторы),

– персональные компьютеры (настольные, переносные),

– периферийное (принтеры, сканеры, источники бесперебойного питания, переносные носители информации),

– коммутационное (модемы, коммутаторы) и линии связи.

Программные средства включают в себя прикладные и системные программы.

КС можно представить в виде узлов, объединенных линиями связи. Каждый такой узел может состоять из нескольких составляющих (программных и аппаратных). Чем больше узлов содержит сеть, тем больше вероятность успешной атаки на систему в целом, так как каждый узел подвержен риску угрозы НСД, а реализация одной из них на любом узле приведет к нарушению целостности системы в целом. В связи с этим не рекомендуется вводить избыточные узлы, узлы, которые не будут задействованы в обработке информации, а на самих узлах необходимо минимизировать количество компонентов.

Серверное оборудование является привлекательным объектом для злоумышленников. Обладая мощными вычислительными ресурсами, оно позволяет получить доступ к большим массивам обрабатываемой информации. Настройкой и эксплуатацией серверов должны заниматься подготовленные специалисты, что также снижает риск появления бреши в системе защиты. Устанавливается такое оборудование в помещение, защищенное от посторонних.

Персональные компьютеры (ПК) сотрудников имеют гораздо больше уязвимостей. Целью атаки на них может быть как непосредственный доступ к ресурсам ПК, так и завладение узлом, посредством которого могут быть атакованы остальные части сети. Сотрудникам, эксплуатирующим ПК, запрещается установка непроверенного программного обеспечения, разглашение паролей, отключение антивирусных программ, что может привести к снижению уровня защищенности КС.

Каналы связи состоят из линий связи и узлов коммутации, в которых находится сетевое оборудование. В отличие от остальных узлов сети, каналы связи часто подвержены несанкционированному воздействию (НСВ), не связанному с действиями злоумышленников. Деструктивные силы природного характера часто приводят к повреждению линий связи и выходу из строя коммутационного оборудования. Для минимизации последствий от такого НСВ должна быть предусмотрена возможность использования резервных каналов.

1.4 Модель нарушителя

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным ресурсам предприятия.

Под атакой на ресурсы корпоративной сети понимается попытка нанесения ущерба информационным ресурсам систем, подключенных к сети. Атака может осуществляться как непосредственно нарушителем, так и опосредованно, при помощи процессов, выполняющихся от лица нарушителя, либо путем внедрения в систему программных или аппаратных закладок, компьютерных вирусов, троянских программ и т. п.

В соответствии с моделью, все нарушители по признаку принадлежности к подразделениям, обеспечивающим функционирование ИС, делятся на внешних и внутренних.

Внешние нарушители

В качестве внешнего нарушителя рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам систем.

К внешним нарушителям могут относиться:

– уполномоченный персонал разработчиков;

– бывшие сотрудники (администраторы или пользователи);

– посторонние лица, пытающиеся получить доступ к информации или техническим средствам.

Предположения о квалификации внешнего нарушителя формулируются следующим образом:

- является высококвалифицированным специалистом в области использования технических средств перехвата информации;
- знает особенности системного и прикладного ПО, а также технических средств ИС;
- знает специфику задач, решаемых ИС;
- знает функциональные особенности работы системы и закономерности хранения, обработки и передачи в ней информации;
- знает сетевое и канальное оборудование, а также протоколы передачи данных, используемые в системе;
- может использовать только серийно изготовляемое специальное оборудование, предназначенное для съема информации с кабельных линий связи и из радиоканалов.

Внутренние нарушители

К внутренним нарушителям могут относиться:

- администраторы (системный администратор, администратор безопасности);
- зарегистрированные пользователи;
- сотрудники посторонних организаций, выполняющие установку, обновления программного обеспечения;
- сотрудники, имеющие санкционированный доступ в помещения, где установлено оборудование.
- обслуживающий персонал (сотрудники охраны, работники инженерно технических служб, уборщики).

Предположения о квалификации внутреннего нарушителя формулируются следующим образом:

- внутренний нарушитель является высококвалифицированным специалистом в области разработки и эксплуатации ПО и технических средств;

– знает специфику задач, решаемых обслуживающими подразделениями ИС предприятия;

– является системным программистом, способным модифицировать работу операционных систем;

– правильно представляет функциональные особенности работы системы и процессы, связанные с хранением, обработкой и передачей критичной информации;

– может использовать как штатное оборудование и ПО, имеющиеся в составе системы, так и специализированные средства, предназначенные для анализа и взлома компьютерных систем.

1.5 Модель угроз

Для надежной защиты системы необходимо, чтобы политики безопасности предусматривали все возможные угрозы и действовали во всех узлах.

Можно выделить восемь наиболее часто реализуемых в настоящее время угроз.

1. Анализ сетевого трафика

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль.

2. Сканирование сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

3. Угроза выявления пароля.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием

специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). Для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д.

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя.

5. Навязывание ложного маршрута сети.

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы.

6. Внедрение ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска.

7. Отказ в обслуживании.

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

а) скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением

пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов.

б) явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д.

в) явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

8. Удаленный запуск приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста.

2. Мероприятия по защите информации в учреждении

2.1 Антивирусный контроль.

Обязательный антивирусный контроль на рабочих станциях. Обязателен автоматический запуск антивирусного монитора и обязательно его автоматическое обновление через Интернет каждую неделю.

2.2 Защита от НСД.

Необходимо поставить аппаратную систему защиты от НСД, которая должна контролировать и разграничивать доступ к каждой рабочей станции и серверу на аппаратном уровне (при загрузке). Система должна быть:

– ОС - независима и выполнена в виде платы к ЭВМ;

– при загрузке идентификация пользователя должна производиться при помощи смарт карты или электронной «таблетки» и при помощи пароля;

– блокировать доступ в сетап всех рабочих станций и серверов всем пользователям кроме администратора;

– блокировать компьютер, если пользователь покинул свое место (либо по нажатию клавиш, либо по таймауту).

2.3 Криптографическая защита данных

Сотрудники учреждения должны сохранять информацию на PGP крипто диске (или на крипто диске иной разработки), разрешенном менеджментом Учреждения.

2.4 Межсетевое экранирование

Межсетевой экран дает возможность решить, две основных задачи:

– контроль и ограничение доступа из внешних источников к внутренним ресурсам сети. Ограничение доступа необходимо при подключении к корпоративной сети, а также при попытках несанкционированного доступа со стороны злоумышленников.

– ограничение доступа пользователей внутренней сети к внешним ресурсам данных. Как правило, это ресурсы, не имеющие прямого отношения к выполнению сотрудниками рабочих функций.

Межсетевой экран выполняет функций по обеспечению информационной безопасности.

Фильтрация трафика. Смысл фильтрации потоков информации состоит в выборочном пропускании через брандмауэр случайных пакетов данных. Определение потенциально опасной информации основывается на загружаемых в файрвол правилах, которые, в свою очередь, определяются политикой

безопасности, принятой Учреждении. Правила, загружаемые в файрвол, обозначают как набор фильтров, каждый из которых отвечает за определенный критерий отбора.

Аутентификация пользователей. Функции, применяемые для фильтрации трафика, – определение какие пакеты данных могут быть пропущены во внутреннюю сеть, а какие нет, при помощи файрвола с тем же успехом используются и для определения уровня доступа пользователей сети. Прежде чем дать пользователю возможность доступа к определенному ресурсу, брандмауэр сначала проводит его аутентификацию (как правило, ввод логина/пароля), затем, на основании полученных данных, – авторизацию (определение прав доступа) и, сопоставляя, права доступа к ресурсу и права доступа пользователя дает возможность воспользоваться ресурсом или запрещает его использование.

Трансляция сетевых адресов. Одна из наиболее важных функций файрвола. Дает возможность скрыть фактический ip-адрес компьютера, работающего в сети интернет от обнаружения. Достигается это тем, что ip-адреса всех пакетов, отсылаемых компьютерами внутренней сети, проходя через файрвол меняются на другой, стандартный и надежный. Реализация данной функции позволяет значительно снизить опасность атаки на компьютеры сети Учреждения, так как для того, чтобы провести ее, злоумышленнику надо знать настоящий ip-адрес компьютера. Кроме этого, использование функции трансляции ip-адресов, дает возможность иметь внутри Учреждения собственную систему адресации ПК, не зависящую от интернет.

Функции посредничества. Реализуются брандмауэром при помощи специальных программ-посредников, запрещающих прямую передачу пакетов между ресурсами внешней и внутренней сети. Таким образом, при выполнении файрволом функций посредничества, при необходимости доступа из одной части сети в другую, первоначально создается соединение с программой-посредником, которая проверяет допустимость запрошенного взаимодействия и, при его допустимости, уже сама устанавливает соединение с нужным ресурсом. Далее, обмен информацией осуществляется только через эту программу-посредник.

Создание такого механизма взаимодействия ресурсов дает возможность решить целый ряд задач: проверка подлинности передаваемых данных, фильтрация потока информации – поиск вирусов, шпионов и т. д., кэширование данных.

2.5 Резервирование данных.

Обязательным является резервирование пользователями важных данных на персональных компьютерах на внутреннем сервере данных Учреждения.

Обязательно наличие бэкап-диска для сервера данных. Бэкап делается либо каждую неделю, либо после серьезных изменений в системе. Необходимо сохранять три цикла генерации бэкапа.

2.6 Протоколирование доступа

При локальном доступе пользователя к рабочей станции ведется лог-файл его посещений (протоколируются все удачные и неудачные попытки входа в систему)

При локальном доступе администратора к серверам ведется лог-файл его посещений (протоколируются все удачные и неудачные попытки входа в систему)

2.7 Физическая безопасность:

1. Файрвол, веб-сервер, сервера IDS и контроля за трафиком и все сервера данных должны находится в отдельном помещении, доступ в которое разрешен только администраторам, у которых есть ключ или магнитная карта к этой комнате (комната обычно закрыта). Необходимо введение отдельной должности администратора безопасности, и все изменения в системах они будут делать только вдвоем: одна часть пароля администратора имеется у ИТ - администратора, вторая - у администратора безопасности.

2. Помещение должно быть оборудовано принудительной вентиляцией и пожарной защитой (полуавтоматической или автоматической) и, возможно, видео наблюдением за действиями администраторов.

3. Обеспечения безопасности ЛВС учреждения

3.1 Общие правила разграничения доступа в ЛВС

1. Каждый персональный компьютер должен иметь "владельца" или "системного администратора", который является ответственным за работоспособность и безопасность компьютера, и за соблюдение всех политик и процедур, связанных с использованием данного компьютера. Основной пользователь компьютера может выполнять эту роль. Эти пользователи должны быть обучены и обеспечены соответствующими руководствами так, чтобы они могли корректно соблюдать все политики и процедуры.

2. Чтобы предотвратить неавторизованный доступ к данным ЛВС, программному обеспечению, и другим ресурсам, находящимся на сервере ЛВС, все механизмы защиты сервера ЛВС должны находиться под монопольным управлением местного администратора и местного персонала Администраторов ЛВС.

3. Чтобы предотвратить распространение злонамеренного программного обеспечения и помочь выполнению лицензионных соглашений о программах, пользователи должны гарантировать, что их программное обеспечение должным образом лицензировано и является безопасным.

4. За все изменения (замены) программного обеспечения и создание резервных копий данных на серверах отвечают Администраторы ЛВС.

5. Каждому пользователю должен быть назначен уникальный идентификатор пользователя и начальный пароль (или другая информация для идентификации и аутентификации), только после того, как закончено оформление надлежащей документации. Пользователи не должны совместно использовать назначенные им идентификаторы пользователя.

6. Пользователи должны аутентифицироваться в ЛВС перед обращением к ресурсам ЛВС.

7. Идентификатор пользователя должен удаляться после продолжительного периода неиспользования.

8. Использование аппаратных средств ЛВС типа мониторов/регистраторов трафика и маршрутизаторов должно быть авторизовано и проводиться под контролем Администраторов ЛВС.

3.2 Особые обязанности для обеспечения безопасности ЛВС учреждения.

1. Пользователи.

Ожидается, что пользователи хорошо осведомлены относительно политики безопасности Учреждения, и других применимых законов, политик, указов и процедур и твердо их придерживаются. Пользователи полностью отвечают за их собственное поведение. В частности, пользователи отвечают за следующее:

1. Отвечают за понимание и соблюдение соответствующих Федеральных законов, политик и процедур министерства, политик и процедур учреждения и других применимых политик безопасности и связанных с ними последствий для ЛВС учреждения.

2. Отвечают за использование доступных механизмов безопасности для защиты конфиденциальности и целостности их собственной информации, когда это требуется.

2.1. Следуют местным процедурами защиты критических данных, а также процедурам безопасности самой ЛВС учреждения. Используют механизмы защиты файлов для поддержания соответствующего управления доступом к файлам.

2.2. Выбирает и использует хорошие пароли. Не записывает паролей, и не раскрывает их другим. Не использует совместно идентификаторы пользователей.

3. Отвечает за помощь другим пользователям, кто будет не в состоянии должным образом использовать доступные механизмы защиты. Помогает защитить собственность других лиц. Уведомляет их относительно незащищенности их ресурсов (например, файлов, идентификаторов).

4. Отвечает за уведомление местного администратора или члена руководства о нарушении защиты или обнаруженном отказе.

5. Отвечает за неиспользование слабых мест АС.

5.1. Не осуществляет намеренного изменения, уничтожения, чтения, или передачи информации неавторизованным способом: не мешает специально получить другим пользователям авторизованный доступ к ресурсам ЛВС и информации в ней.

5.2. Предоставляет правильную информацию для идентификации и аутентификации, когда это требуется, и не пытается угадать подобную информацию для других пользователей.

6. Отвечает за гарантию выполнения резервного копирования данных и программного обеспечения находящегося на жестком диске их собственного автоматизированного рабочего места.

7. Отвечает за понимание принципов работы злонамеренного программного обеспечения, методов, с помощью которых оно вносится и распространяется, и уязвимых мест, которые используются злонамеренным программным обеспечением и неавторизованными пользователями.

8. Отвечает за знание и использование соответствующих политик и процедур для предотвращения, обнаружения, и удаления злонамеренного программного обеспечения.

9. Отвечает за знание того, на что нужно обращать внимание при работе в определенных системах и конкретных программах, чтобы обнаружить признаки их необычной работы, и что нужно сделать или с кем связаться для получения дополнительной информации.

10. Отвечает за использование программно-аппаратных средств защиты, которые доступны для защиты системы от злонамеренного программного обеспечения.

11. Отвечает за знание и использование процедур по обеспечению непрерывной работы для сдерживания и восстановления при потенциальных инцидентах.

2. Функциональное руководство.

Функциональное руководство (и управляющие более высокого уровня) отвечают за разработку и выполнение эффективных политик безопасности, которые отражают специфические цели ЛВС учреждения. Они полностью отвечают за обеспечение того, что защита информации и линий связи является и остается важной и критической целью в повседневной деятельности. В частности функциональное руководство отвечает за следующее:

1. Отвечает за проведение эффективного управления риском для того, чтобы обеспечить основу для формулирования разумной политики. Управление риском требует идентификации ценностей, которые нужно защитить, определения уязвимых мест, анализа риска их использования и реализации рентабельных средств защиты.

2. Отвечает за гарантию того, чтобы каждый пользователь получил, как минимум, копию политики безопасности и местного руководства (если таковые есть в наличии) до внесения его в списки пользователей АС.

3. Отвечает за осуществление программы обучения основам безопасности для пользователей, чтобы можно было гарантировать знание ими местной политики безопасности и правил работы на компьютере.

4. Отвечает за гарантию того, что весь персонал в пределах операционной единицы организации знает эту политику и отвечает за включение ее в инструктажи по компьютерной безопасности и программы обучения .

5. Отвечает за информирование местного администратора и администраторов ЛВС об изменениях в статусе любого служащего, который использует ЛВС учреждения. Это изменение статуса может включать переход из организации в организацию в одном ведомстве, переход из отдела в отдел, или окончание службы в учреждении.

6. Отвечает за гарантию того, что пользователи понимают природу злонамеренного программного обеспечения, понимают, как оно вообще распространяется, и какие программно-аппаратные средства защиты должны использоваться против него.

3. Администраторы Локальной Вычислительной Сети (ЛВС)

Предполагается, что администраторы ЛВС (или назначенный для этого персонал) претворяет (в части их касающейся) местные политики безопасности, так как это связано с применением программно-аппаратных средств защиты, архивированием критических программ и данных, управлением доступом и защитой оборудования ЛВС. В частности, администраторы ЛВС отвечают за следующее:

1. Отвечают за корректное применение доступных механизмов защиты для осуществления местных политик безопасности.

2. Отвечает за уведомление руководства о работоспособности существующих политик и любых технических соображениях, которые могли бы улучшить их эффективность.

3. Отвечает за защищенность среды ЛВС внутри организации и интерфейсов с глобальными сетями.

4. Отвечает за оперативное и эффективное улаживание происшествий с компьютерной безопасностью.

4.1. Уведомляет местных администраторов о проникновении злоумышленника в ЛВС , помогает другим местным администраторам улаживать происшествия с безопасностью.

4.2. Сотрудничает с местными администраторами при выявлении нарушителя и помогает им это сделать.

5. Отвечает за использование надежных и доступных средств аудирования для облегчения обнаружения нарушений безопасности.

6. Отвечает за проведение своевременных проверок системных журналов серверов ЛВС.

7. Отвечает за отслеживание информации о политиках безопасности и приемах обеспечения безопасности в других организациях и, когда это необходимо, информирование местных пользователей и уведомление руководства об изменениях или новых разработках.

8. Отвечает за крайнюю осторожность и корректность при применении им своих полномочий и привилегий. Безопасность пользователей должна всегда стоять на первом месте.

9. Отвечает за разработку соответствующих процедур и издание инструкций по предотвращению, обнаружению, и удалению злонамеренного программного обеспечения, соответствующих руководящим принципам, содержащимся в этом документе.

10. Отвечает за своевременное создание резервных копий всех данных и программного обеспечения на серверах ЛВС.

11. Отвечает за выявление и рекомендацию пакетов программ для обнаружения и удаления злонамеренного программного обеспечения.

12. Отвечает за разработку процедур, позволяющих пользователям сообщать о компьютерных вирусах и других инцидентах и отвечает за уведомление потенциально затрагиваемых лиц о возможной угрозе им.

13. Отвечает за скорое уведомление соответствующей группы улаживания происшествий с компьютерной безопасностью обо всех инцидентах, включая выявление злонамеренного программного обеспечения.

14. Отвечает за оказание помощи при определении источника злонамеренного программного обеспечения и зоны его распространения.

15. Отвечает за обеспечение помощи в удалении злонамеренного программного обеспечения.

16. Отвечает за проведение периодического анализа для того, чтобы гарантировать, что соблюдаются надлежащие процедуры безопасности, включая те, которые предназначены для защиты от злонамеренного программного обеспечения.

4. Местные Администраторы

Ожидается, что местные администраторы (или назначенный персонал) будут использовать доступные службы и механизмы защиты ЛВС на сервере, за который они отвечают, чтобы поддерживать и претворять в жизнь применимые политики и процедуры безопасности. В частности, местные администраторы отвечают за следующее:

1. Отвечают за управление привилегиями доступа всех пользователей к данным, программам и функциям.

2. Отвечают за контроль за всеми связанными с защитой событиями и за расследование любых реальных или подозреваемых нарушений там, где это уместно. В соответствующих случаях отвечают за уведомление и координацию

действий с Администраторами ЛВС по контролю или расследованию событий, связанных с нарушением безопасности.

3. Отвечает за поддержание и защиту программного обеспечения и соответствующих файлов на сервере ЛВС, используя доступные механизмы и процедуры защиты.

4. Отвечает за сканирование сервера ЛВС антивирусным программным обеспечением через регулярные интервалы времени для гарантии того, что никакому вирусу не удалось разместиться на сервере ЛВС.

5. Отвечает за назначение уникального имени и начального пароля (или другой идентификационной и аутентификационной информации) каждому пользователю только после того, как будет оформлена надлежащая документация.

6. Отвечает за быстрое уведомление соответствующего персонала группы улаживания происшествий с компьютерной безопасностью обо всех инцидентах, включая злонамеренное программное обеспечение;

6.1. Уведомляет Администраторов ЛВС о проникновении в ЛВС , помогает другим местным администраторам улаживать нарушение безопасности.

6.2. Сотрудничает с другими местными администраторами и Администраторами ЛВС в поиске нарушителя и помогает им это сделать.

7. Отвечает за обеспечение помощи при выявлении источника злонамеренного программного обеспечения и зоны его распространения.

Начальник отдела информатизации
и электронного межведомственного
взаимодействия В. Черкесов