

бюджетное профессиональное
образовательное учреждение
Вологодской области
«Великоустюгский
многопрофильный колледж»

УТВЕРЖДЕН
приказом директора
колледжа

от 24.05.2022 г. № 236



ПЛАН

«24» 05 2022 г. № 16

г. Великий Устюг

защиты информационных ресурсов от несанкционированного доступа

Назначение Плана

План защиты информационных ресурсов от несанкционированного доступа (далее – План) определяет организацию, порядок осуществления работ, основные требования и рекомендации, способы и средства защиты информации, циркулирующей в ИС, технических средствах и помещениях бюджетного профессионального образовательного учреждения Вологодской области «Великоустюгский многопрофильный колледж» (далее – учреждение), и является основным руководящим документом для сотрудников учреждения (в части их касающейся).

Настоящий План разработан на основании действующих законодательных актов и руководящих документов.

ИС подвергаются различным видам рисков, начиная с потери данных в результате ошибок пользователей и кончая стихийными бедствиями. Наиболее серьезные угрозы, вызывающие прекращение работы системы, такие как стихийные бедствия, обычно рассматриваются в плане ликвидации последствий аварии. Другие угрозы безопасности связаны со злонамеренной технической активностью (такой как компьютерные вирусы или действия нарушителей информационной безопасности).

Назначением настоящего Плана является документирование согласованных решений по предотвращению, выявлению, реагированию и ликвидации последствий нарушения режима информационной безопасности. Комплексный подход реализуется за счет охвата всех уровней управления: административного, процедурного и программно-технического.

Основные положения Плана

Подготовка Плана защиты информационных ресурсов учреждения от НСД и контроль его исполнения осуществляется системным администратором. Внесение изменений и дополнений в настоящий План осуществляется по инициативе

заинтересованных структурных подразделений после согласования и утверждения директором учреждения. Ответственность за исполнение положений Плана возлагается на пользователей и обслуживающий персонал ИС учреждения (в части, их касающейся).

План состоит из пяти частей.

Первая часть Плана определяет состав и последовательность административных мероприятий, проводимых с целью организации защиты от НСД к информации. Ее цель – создать условия и подготовить персонал ИС учреждения (в части их касающейся) к проведению работ по предотвращению, выявлению и реагированию на нарушения безопасности, а также по ликвидации последствий нарушений безопасности. Для успешного проведения этих мероприятий необходимо, чтобы была правильно распределена ответственность между должностными лицами, отвечающими за обеспечение информационной безопасности, и чтобы каждый сотрудник знал свои должностные обязанности. Кроме того, необходимо разработать, протестировать и распространить среди персонала инструкции и регламенты по обеспечению информационной безопасности, провести работу с пользователями и проверить наличие необходимых ресурсов, в том числе и специализированных СЗИ от НСД.

Во второй части Плана описывается состав мероприятий и порядок действий по предотвращению нарушений безопасности. Необходим непрерывный контроль состояния ИС, действий пользователей, своевременное выявление и ликвидация уязвимостей в системе защиты. Этим целям служат мониторинг и аудит безопасности. Под мониторингом понимается отслеживание опасных состояний системы и подозрительных действий пользователей, производимое в реальном времени, либо строго периодически. Аудит предполагает проведение регулярных проверок процесса функционирования ИС посредством анализа журналов регистрации событий системного и прикладного ПО.

Третья часть Плана содержит пошаговые инструкции по анализу нарушений безопасности. Анализ позволяет установить, действительно ли нарушение имеет (имело) место, была ли попытка НСД успешной, а также насколько серьезно система была скомпрометирована.

Четвертая часть Плана определяет действия по реагированию на нарушения безопасности, предусматривающие применение мер процедурного и программно-технического уровня.

Пятая часть Плана определяет систему мероприятий по ликвидации последствий нарушений безопасности. Она содержит рекомендации по организации восстановительных работ, переводу системы в защищенное состояние, анализу и ликвидации уязвимостей системы защиты.

Организация режима информационной безопасности

Назначение ролей и распределение ответственности. Права и обязанности

В данном разделе определяются обязанности системного администратора, инженеров и программиста учреждения по предупреждению, реагированию и ликвидации последствий нарушений безопасности.

Организация режима информационной безопасности и эксплуатация СЗИ ИС колледжа осуществляется инженером и программистом, выполняющими следующие задачи:

- классификация и определение степени критичности и конфиденциальности информационных ресурсов ИС;
- анализ рисков, связанных с нарушениями информационной безопасности;
- выбор адекватных методов и средств защиты информации, применяемых для защиты ИС;
- изучение, сравнительный анализ и принятие решений о целесообразности использования тех или иных программно-технических средств защиты информации;
- разработка и контроль выполнения планов, процедур, регламентов и инструкций по обеспечению информационной безопасности;
- администрирование и сопровождение комплекса СЗИ, входящих в состав ПИБ;
- выявление возможных каналов утечки информации и разработка системы мер по их устранению;
- проведение профилактических мероприятий по предотвращению нарушений информационной безопасности, проведение инструктажей пользователей и обслуживающего персонала ИС, повышение их осведомленности в вопросах обеспечения информационной безопасности;
- проведение предварительного тестирования СЗИ, системного и прикладного ПО на предмет адекватной реализации механизмов безопасности и соответствия требованиям по защите информации;
- мониторинг внешних источников информации, с целью своевременного выявления новых уязвимостей, эксплуатируемого ПО;
- обеспечение режима конфиденциальности сведений ограниченного распространения.

В соответствии с должностными инструкциями системного администратора, инженеров и программиста учреждения для выполнения ими своих обязанностей по обеспечению информационной безопасности они наделяются следующими правами.

Системный администратор вправе:

- знакомиться с проектами решений администрации учреждения, касающимися деятельности ИС;
- осуществлять взаимодействие с руководителями всех структурных подразделений учреждения по вопросам защиты информации;
- подписывать и визировать документы в пределах своей компетенции.
- вносить на рассмотрение администрации учреждения представления о назначении, перемещении и освобождении от занимаемых должностей подчиненных ему работников, предложения о поощрении отличившихся работников, предложения о привлечении к материальной и дисциплинарной ответственности виновных в утечке информации, составляющей государственную и коммерческую тайну;
- запрашивать и получать от руководителей структурных подразделений учреждения, специалистов и рабочих информацию и материалы, необходимые для организации работы ИС.

Инженер и программист учреждения имеют право:

- осуществлять взаимодействие с руководителями всех структурных подразделений учреждения по вопросам защиты информации;
- подписывать и визировать документы в пределах своей компетенции;
- запрашивать лично или по поручению своего непосредственного руководителя от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей;
- в пределах своей компетенции сообщать непосредственному руководителю о всех выявленных в процессе осуществления должностных обязанностей недостатках в деятельности учреждения (ее структурных подразделений) и вносить предложения по их устранению;
- привлекать специалистов отдельных структурных подразделений к решению задач, возложенных на него (если это предусмотрено положениями о структурных подразделениях, если нет - то с разрешения их руководителей);
- требовать от системного администратора или администрации учреждения оказания содействия в исполнении своих должностных обязанностей и прав.

Распределение обязанностей

Согласно регламентам проведения административных мероприятий, различают пять областей администрирования:

- системное администрирование;
- сетевое администрирование;
- администрирование приложений;
- администрирование средств защиты информации;
- аудит безопасности.

1. Системный администратор производит настройку системного ПО, осуществляет мониторинг состояния вычислительных систем, входящих в состав ИС, выполняет анализ производительности сети, настройку средств защиты информации, встроенных в системное ПО, резервное копирование информации и ее восстановление после сбоев.

Деятельность системного администратора включает в себя:

- администрирование файловых систем:
 - анализ и планирование файловых систем;
 - создание файловых систем;
 - монтирование файловых систем;
 - копирование файловых систем;
 - проведение настройки встроенных с системное ПО средств защиты информации в соответствии с предоставляемыми пользователям правами (совместно с инженерами и программистом учреждения);
 - резервирование и восстановление информации;
 - контроль использования дискового пространства;
 - консультирование пользователей по вопросам функционирования системного ПО.

Системный администратор производит диагностику и поиск ошибок:

- начальной загрузки и закрытия системы;
- проверку целостности файловой системы;
- анализ аварийных дампов;

- диагностирование проблем с аппаратурой и замена испорченной аппаратуры.

Системный администратор выполняет добавление устройств и драйверов в систему, форматирование дисков и разделение их на разделы. Производит установку нового системного программного обеспечения и пакетов программных коррекций для ОС.

Совместно с инженерами и программистом учреждения проводит анализ случаев НСД к ресурсам ИС.

В обязанности системного администратора входит сопровождение и поддержка в актуальном состоянии документации на ИС.

2. Инженеры учреждения отвечают за выполнение административных мероприятий по конфигурированию активного сетевого оборудования и СКС.

Деятельность инженеров включает в себя:

- анализ и планирование развития кабельной структуры и сетевого оборудования;

- настройку и конфигурирование коммутаторов, маршрутизаторов, мостов, концентраторов и т.п.;

- мониторинг производительности сети (в части СКС и сетевого оборудования);

- устранение неисправностей в функционировании сети (в части СКС и сетевого оборудования);

- организацию замены и ремонта вышедшего из строя оборудования;

- консультирование пользователей по вопросам, касающимся его функциональных обязанностей;

- проведение настройки сетевого оборудования (совместно с программистом и системным администратором);

- организация мероприятий по надежному размещению сетевого оборудования. Данные мероприятия направлены на исключение возможности несанкционированного доступа к сетевому оборудованию и СКС;

- контроль действия пользователей с целью исключения возможности несанкционированного подключения к ИС учреждения различных технических средств;

Совместно с системным администратором и программистом учреждения проводят анализ случаев НСД к ресурсам ИС.

3. Программист отвечает за выполнение административных мероприятий по установке, настройке и поддержанию в работоспособном состоянии прикладного программного обеспечения, эксплуатируемого в организации.

Деятельность программиста включает в себя:

- участие в работе по созданию приложений. Программист в силу своих функциональных обязанностей обязан принимать участие в обсуждении всех этапов создания приложения. Он должен четко знать алгоритм обработки данных приложением, особенности настройки и эксплуатации, методы аутентификации и разграничения доступа, реализованные в приложении (в случае, если это было реализовано разработчиками приложения);

- установку и настройку серверной части приложения;

- установку и настройку клиентской части на АРМ пользователей;

- консультации с пользователями по вопросам, касающимся эксплуатации, установленных приложений;

- совместно с инженерами, на основании заявок по предоставлению доступа к ресурсам, производит настройку средств защиты информации;

- ведение и поддержание в актуальном состоянии перечня задач и эксплуатационной документации к ним. Для каждой задачи должен быть составлен список пользователей, работающих с ней, а также перечень ресурсов, к которым эти пользователи допущены;

- следит за функционированием приложений. В случае сбоев в процессе работы приложения проводит анализ причин и самостоятельно, либо совместно с разработчиком, устраняет их;

- осуществляет мониторинг производительности установленных приложений;

Совместно с системным администратором и инженерами учреждения проводит анализ случаев НСД к ресурсам ИС.

4. Инженеры отвечают за выполнение административных мероприятий по установке, настройке, поддержке в работоспособном состоянии средств защиты информации, эксплуатируемых в ИС учреждения.

Деятельность инженеров включает в себя:

- реализацию требований информационной безопасности, принятой в учреждении. Инженеры координируют деятельность других работников с целью достижения необходимого уровня защиты информации в ИС;

- анализ состояния информационной безопасности ИС;

- анализ используемых средств и методов защиты информации;

- планирование развития подсистемы информационной безопасности;

- осуществление настройки средств защиты информации, эксплуатируемых в ИС. Настройки выполняются в соответствии с предоставляемыми пользователям сервисами и правами доступа. При выполнении настроек инженеры должны руководствоваться принципом минимизации привилегий – «что не разрешено, то запрещено»;

- составление и поддержание в актуальном состоянии документации по размещению и конфигурации средств защиты информации;

- для каждого пользователя заводит имя и регистрирует пароль в соответствии со схемой, принятой в учреждении;

- на основании письменной заявки каждому пользователю, в соответствии с выполняемыми функциональными обязанностями, предоставляется доступ к ресурсам и сервисам ИС. Инженер выполняет настройку средств защиты в соответствии с заявкой.

- ведение и поддержание в актуальном состоянии списка пользователей, допущенных к работе в ИС, а также перечня предоставленных пользователям прав на доступ к ресурсам и сервисам;

- постоянный контроль за работоспособностью средств защиты информации. В случае неисправности либо ненадлежащего функционирования действует в соответствии с правилами, принятыми в учреждении;

- мониторинг средств защиты (постоянно). При выявлении попытки НСД к информации проводит анализ и в случае необходимости докладывает об этом своему непосредственному начальнику;

- в случае НСД к информации инженеры докладывают о факте НСД системному администратору и совместно с программистом проводят анализ ситуации. В результате анализа вырабатываются предложения по предотвращению повторного НСД к информации.

5. Системный администратор отвечает за выполнение административных мероприятий по установке, настройке, поддержке в работоспособном состоянии средств аудита, эксплуатируемых в ИС учреждения.

Средства аудита предназначены для контроля и обнаружения различных угроз, которым подвергается ИС и ее информационные ресурсы, а также для реагирования на эти угрозы в реальном масштабе времени.

Деятельность системного администратора включает в себя:

- установку и настройку средств аудита. Настройки выполняются в соответствии с Политикой информационной безопасности, принятой в учреждении;

- анализ состояния информационной безопасности ИС;

- составление и поддержание в актуальном состоянии документации по размещению и конфигурации средств аудита;

- осуществление постоянного контроля за работоспособностью средств аудита информационной безопасности ИС. В случае неисправности либо ненадлежащего функционирования этих средств действует в соответствии с правилами, принятыми в учреждении;

- в случае обнаружения угрозы либо факта осуществления НСД к информации системный администратор совместно с инженерами и программистом проводит анализ ситуации. В результате анализа вырабатываются предложения по ликвидации угрозы;

Совместно с инженерами и программистом учреждения проводит анализ случаев НСД к ресурсам ИС.

Определение рабочих профилей пользователей ИС

На этапе настройки системы аудита безопасности учреждения определяются рабочие профили пользователей ИС.

Рабочий профиль пользователя – это набор характеристик, позволяющих инженеру и системам автоматического выявления нарушений безопасности отождествлять пользователей системы с производимыми ими действиями и выявлять подозрительную активность, несвойственную данным пользователям.

Рабочий профиль включает следующие характеристики:

- выполняемые функции;

- приложения, с которыми работает пользователь;

- группы, членами которых является пользователь;

- используемый командный интерпретатор;

- системное окружение, в котором работает пользователь;

- уровень пользовательских полномочий;

- роли, присвоенные пользователю в СУБД;

- режим работы;

- стиль работы и т. п.

Процедуры по предупреждению компьютерного мошенничества выполняются регулярно инженерами, программистом и системным администратором. Они включают в себя фиксацию и анализ критических отклонений в поведении пользователей ИС учреждения от стандартных параметров, определяющих их типичное поведение и содержащихся в профилях пользователей. Выявление критических отклонений в поведении пользователей осуществляется по результатам анализа данных аудита безопасности.

Требования безопасности, предъявляемые к пользователям ИС

Пользователями ИС являются сотрудники учреждения, зарегистрированные соответствующим образом в системе и получившие права на доступ к ресурсам ЛВС в соответствии с функциональными обязанностями.

Все пользователи ИС должны быть ознакомлены с содержанием данного Плана и других документов, регламентирующих работу в ИС, в части, их касающейся. За нарушение установленных правил работы в ИС учреждения пользователи несут персональную ответственность.

Всем пользователям ИС присваивается уникальное имя и предлагается выбрать пароль. При регистрации в системе пользователю необходимо ввести свое уникальное имя. Пароль служит доказательством того, что пользователь является именно тем, за кого себя выдает. Имя и пароль пользователи обязаны держать в секрете, никому не сообщать и нигде не записывать.

При выборе пароля пользователь должен руководствоваться следующими основными правилами:

- выбирать пароли длиной не менее семи символов;
- при выборе паролей не следует использовать: даты, фамилии, инициалы, регистрационные номера автомобилей, названия организаций и населенных пунктов, номера телефонов, пользовательские идентификаторы, повторяющиеся последовательности символов, слова русского или английского языков и т.п.;
- осуществлять регулярную смену паролей (через каждые 90 дней), избегать повторного использования старых паролей;
- для привилегированных пользователей необходима более частая смена паролей (через каждые 45 дней);
- изменять пароль каждый раз, когда есть подозрение о его компрометации;
- не включать пароли в сценарии для автоматического входа в системы (например, в макросы).

Установку системного и прикладного программного обеспечения на рабочем месте пользователя, его конфигурирование выполняют инженеры. Пользователю запрещается самостоятельно устанавливать любое ПО на свое рабочее место. В случае необходимости установки дополнительных программных средств пользователь подает письменную заявку системному администратору. После рассмотрения заявки системным администратором и в случае положительного решения инженер производит установку необходимых программ.

Пользователю запрещается самостоятельно вскрывать компьютер, производить замену или установку аппаратной части. Пользователь несет персональную ответственность за сохранность защитных знаков, которыми опечатан компьютер. В случае необходимости замены вышедшего из строя

аппаратного обеспечения либо установки дополнительного пользователь обращается с письменной заявкой к системному администратору. После рассмотрения заявки производятся работы в соответствии с правилами, принятыми в учреждении.

Пользователь ИС обязан использовать АРМ и предоставленные ему сервисы только для выполнения своих функциональных обязанностей. Не допускается выполнение посторонних работ, обмен информацией с сетью Интернет в обход принятой в учреждении технологии. Категорически запрещается создавать дополнительные каналы выхода в сеть Интернет (устанавливать внешние модемы, подключаться через стороннего провайдера и т.п.).

При работе в сети Интернет запрещена загрузка и установка на свой компьютер программного обеспечения. Не разрешается использование почтовых ящиков, предоставляемых сторонними провайдерами.

Пользователь не имеет права сообщать посторонним лицам техническую информацию по конфигурации и настройке ИС (состав ЛВС, количество компьютеров, их модели, используемые средства защиты, IP-адреса, имена доменов, почтовых ящиков и т.д.).

Пользователь обязан знать правила и уметь работать с антивирусными программами, установленными на компьютер. Вся входящая информация перед открытием должна проверяться на наличие вирусов. Пользователь обязан проводить периодическое тестирование своего АРМ. Периодичность тестирования программного обеспечения устанавливается в соответствии с антивирусной политикой. В случае обнаружения компьютерного вируса, необычной работы компьютера либо приложения пользователь обязан сообщить об этом непосредственному начальнику и администратору, и действовать в соответствии с их указаниями.

Пользователи должны обеспечить надлежащую защиту оборудования, оставленного без присмотра. Оборудование, установленное на рабочих местах пользователей (например, рабочие станции или файловые серверы), может потребовать организации защиты от НСД.

Пользователи должны знать процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Предлагаются следующие рекомендации:

- завершить сеансы связи по окончании работы, если их нельзя защитить посредством соответствующей блокировки;
- использовать логическое отключение от серверов по окончании сеанса связи. Не ограничиваться только выключением ПК или терминала;
- защитить неиспользуемые ПК или терминалы путем блокировки ключом или другими средствами контроля доступа.

По окончании работы с компьютером пользователь должен выключить его.

Назначение ответственных за внесение изменений в системное ПО, распространение версий и изменение конфигурации

Процесс контроля за внесением изменений, распространением версий и изменением конфигурации ПО касается инженеров, программиста и системного администратора учреждения.

Назначение ответственных за связь с другими организациями и определение их обязанностей

Политика информационной безопасности должна определять процедуры для взаимодействия с другими организациями, в число которых входят правоохранительные органы, а также другие организации, затронутые инцидентом.

Должны быть назначены сотрудники, ответственные за связь с этими организациями. Во избежание ситуаций, когда невозможно связаться с ответственным сотрудником, необходимо иметь более одного человека для каждой области ответственности.

Политика информационной безопасности должна определять также следующие вопросы:

- виды контактов с общественностью и ответственного за связь с прессой;
- в каких ситуациях следует обращаться в правоохранительные органы;
- виды информации, которая может быть доступна общественности и другим организациям.

Назначение ответственных за проведение мониторинга внешних источников информации

Помимо определения того, с какими организациями нужно установить связь в случае нарушения безопасности, политикой информационной безопасности также определяются сотрудники, ответственные за проведение мониторинга внешних источников информации с тем, чтобы оставаться в курсе текущих исследований в этой области, актуальных вопросов и проблем.

Ответственные сотрудники должны использовать списки рассылки и группы новостей для участия в обсуждении представляющих интерес вопросов информационной безопасности, используя ресурсы сети Интернет.

Процедура внесения изменений в системное ПО, процедура управления распространением версий и внесения конфигурационных изменений

Внесение изменений в системное ПО проводится в случаях установки программных коррекций используемого ПО, установки новых версий ОС и СУБД.

Допускается эксплуатация только лицензионного ПО, приобретенного непосредственно у разработчика, либо его официального представителя. Перед установкой ПО на действующую ИС необходимо провести тестовые испытания ПО на стенде. Факт внесения изменений документируется для каждого СВТ, эксплуатируемого в ИС, с указанием конфигурационных параметров установленного ПО.

Ведение журналов по внесению изменений в системное и прикладное ПО ИС учреждения возлагается на инженеров и программиста учреждения.

Планирование обучения и собраний персонала ИС

Необходимо спланировать процесс обучения администраторов и пользователей ИС действиям по предотвращению и реагированию на нарушения безопасности, а также обсудить с ответственными сотрудниками отдельные аспекты Политики информационной безопасности. Для этого необходимо:

Разработать планы и графики проведения занятий с инженерами и пользователями ИС с целью разъяснения степени ответственности и области компетенции каждого сотрудника при обеспечении информационной безопасности, а также действий персонала по реагированию на нарушения безопасности. Предусмотреть проведение собраний инженеров и пользователей ИС для обсуждения требований политики информационной безопасности. Важно, чтобы эти требования не создавали пользователям препятствий при выполнении их должностных обязанностей, иначе будет существовать устойчивая тенденция обойти ограничения, накладываемые политикой информационной безопасности. Квалификация персонала должна быть подтверждена соответствующими сертификатами и периодически проверяться при проведении плановых аттестаций сотрудников.

Восстановление работоспособности ИС

Мероприятия по восстановлению работоспособности ИС в случае аварии предусматривают возможность замены пришедших в негодность технических средств, восстановление или переустановку ПО, восстановление информации с архивных копий, либо носителей резервного копирования в соответствии с регламентом резервного копирования и восстановления данных.

Подготовка пользователей ИС к решению проблем, связанных с обеспечением информационной безопасности

Подготовка списков контактных лиц

Необходимо подготовить и распространить среди пользователей ИС и ответственных лиц списки контактных лиц (телефоны, факсы, адреса электронной почты, номера пейджеров и т.п.) для связи в случае выявления фактов нарушения информационной безопасности.

Подготовка рекомендаций по обеспечению информационной безопасности

Необходимо распространить среди пользователей ИС и ответственных лиц рекомендации по обеспечению информационной безопасности в части:

1. Использования лицензионного и только проверенного ПО.

К эксплуатации в ИС учреждения допускается только лицензионное ПО, приобретенное непосредственно у разработчика либо его официального представителя. Перед вводом в эксплуатацию ПО должно проходить тестирование (проверку работоспособности и функционального соответствия) на стенде. В случае успешного прохождения тестирования ПО допускается к эксплуатации.

2. Предотвращения и ликвидации последствий действия компьютерных вирусов.

Используемые средства антивирусной защиты должны выполнять проверку всей входящей и исходящей электронной почты, а также файлов, хранящихся на серверах и рабочих станциях пользователей ИС учреждения.

Допускается использование только лицензионных средств антивирусной защиты, с регулярно обновляемыми базами данных антивирусных сигнатур. Периодичность проведения проверок определяется в зависимости от критичности информации, хранимой на СВТ, и интенсивностью информационного обмена.

При обнаружении компьютерного вируса пользователь обязан доложить об этом системному администратору. После чего под руководством системного администратора произвести удаление вируса и восстановление информации с использованием антивирусных средств.

Каждый случай заражения вирусом должен быть тщательно проанализирован и результаты анализа представлены программисту.

3. Требования и рекомендации по выбору паролей и использованию другой аутентификационной информации.

4. Правила пользования сетевыми сервисами.

Пользователям предоставляются сетевые сервисы в зависимости от решаемых задач. Набор сервисов должен быть минимален. Настройка рабочих мест пользователей должна производиться под контролем инженеров и программиста учреждения. Самовольно изменять конфигурацию категорически запрещается.

Тестирование процедур и регламентов по обеспечению информационной безопасности

Необходимо тщательно протестировать отдельные процедуры и регламенты, предусмотренные настоящим Планом, отработать последовательность действий персонала. При тестировании следует обращать особое внимание на подготовленность ответственных сотрудников к выполнению регламентов и процедур, наличие необходимого инструментария для обслуживания системы и других программно-аппаратных ресурсов, а также соответствие настоящего Плана, процедур и регламентов реальному положению дел.

Проверка наличия и работоспособности специализированных программно-технических средств защиты информации

Необходимо проверить наличие и работоспособность специализированных программно-технических средств защиты информации, таких как средства мониторинга, аудита безопасности, межсетевые экраны, антивирусные средства и т.п.

Заключение стратегических союзов с другими предприятиями и/или организациями

В случае необходимости должны быть заключены стратегические союзы, соглашения и договора с другими предприятиями или организациями (поставщиками, сервисными центрами, консалтинговыми фирмами и т.п.) с целью

проведения мероприятий по восстановлению работоспособности ИС с привлечением дополнительных средств союзников и расследования нарушений безопасности.

Предупреждение нарушений безопасности

Мониторинг состояния ИС

Мониторинг состояния ИС проводится регулярно в соответствии с планом.

Мониторинг функционирования аппаратных компонентов

В соответствии с утвержденным регламентом должен систематически проводиться мониторинг работоспособности аппаратных компонентов ИС. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы ЛВС, активное сетевое оборудование) должны контролироваться постоянно.

Управление паролями пользователей

Пароль является одним из основных средств аутентификации в ИС учреждения. Зарегистрировавшись на сервере под конкретным паролем, пользователь получает доступ к тем ресурсам, к которым ему предоставлены права доступа в соответствии с выполняемыми функциями. Узнав имя пользователя и его пароль, злоумышленник может выполнять действия и просматривать информационные ресурсы от имени легального пользователя. В данной ситуации возможны как финансовые потери от действий злоумышленника, так и потеря доверия со стороны клиентов и партнеров колледжа.

Возможно использование двух схем выработки паролей:

1. Пароли генерируются для каждого пользователя с использованием специального ПО.

2. Каждый пользователь самостоятельно выбирает для себя пароль.

В первой схеме, с использованием специализированного ПО, гарантируется необходимая стойкость пароля (длина, уникальность, необходимая мощность алфавита, невозможность подбора методом полного перебора и т.д.). Но возникают трудности для пользователей с запоминанием сгенерированных паролей.

Кроме того, используя данную схему, необходимо решить ряд организационных вопросов:

- процедуру выдачи паролей пользователям;
- способ хранения носителя с выданным паролем (например, индивидуальный сейф в охраняемом помещении);
- контроль использования носителя и его дальнейшее уничтожение после смены пароля.

Данную схему целесообразно применять при наличии отлаженных механизмов режимного делопроизводства.

Вторая схема лишена перечисленных недостатков, но при ее реализации не гарантирована необходимая стойкость пароля (по статистике около 80% пользователей используют очень простые, легко ассоциируемые с самим пользователем пароли).

Ниже приведены общие правила работы с паролями, обязательные для использования в ИС учреждения.

1. Идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя.
2. Пароли должны состоять как минимум из 7 символов.
3. Пароль должен быть трудно угадываемым. Пароль не должен совпадать с именем пользователя. Паролем не может быть слово на русском или иностранном языках. В пароле не должна в явном виде использоваться информация, ассоциируемая с владельцем пароля (имя, фамилия, дата рождения, номер автомобиля, имена близких родственников и т.п.).
4. Пароли должны держаться в секрете, то есть не должны сообщаться другим людям, не должны вставляться в тексты программ, и не должны записываться на бумаге либо на обратной стороне клавиатуры и т.п.
5. Пароли должны меняться каждые 90 дней (или через другой период, определенный ответственным лицом). Большинство систем могут заставить принудительно поменять пароль через определенное время и предотвратить использование того же самого или легко угадываемого пароля. Для привилегированных пользователей необходима более частая смена паролей (через каждые 45 дней).
6. Пользователи и инженеры ИС обязаны изменять пароль каждый раз, когда есть подозрение о его компрометации.
7. Средства защиты должны быть сконфигурированы таким образом, чтобы учетные записи пользователей блокировались после 3 неудачных попыток входа в систему. Все случаи неверно введенных паролей должны быть записаны в системный журнал, используемый для анализа попыток проникновения в систему.
8. При успешном входе в систему должны отображаться дата и время последнего входа в систему.
9. Сеансы пользователей с сервером должны блокироваться после 15-минутной неактивности пользователя (или по истечении другого указанного периода времени). Для возобновления сеанса должен снова требоваться ввод пароля.
10. Учетные записи пользователей должны блокироваться после определенного времени неиспользования.
11. Должно производиться периодическое тестирование специальными программными средствами (взломщиками паролей) процедуры выбора паролей для случайно выбранных пользователей. Целью тестирования является выявление легко угадываемых паролей.
12. Не следует включать пароли в сценарии для автоматического входа в системы (например, в макросы).
13. Рекомендуются использовать однонаправленные хэш-функции и алгоритмы шифрования для защиты пользовательских паролей, хранимых в системе.

Пользователи, в результате действий (ненадлежащим образом выбран пароль) которых произошло раскрытие критичной информации, несут ответственность в соответствии с правилами, установленными в учреждении.

Контроль за выполнением настоящих рекомендаций возлагается на инженеров учреждения. Для усиления политики управления паролями и контроля надежности пользовательских паролей инженерам необходимо:

- установить программу, осуществляющую проверку пользовательских паролей на очевидность с целью выявления слабых паролей, которые легко угадать, или дешифровать с помощью специализированных программных средств (взломщиков паролей), или использовать встроенные системные средства;

- периодически использовать взломщики паролей для выявления слабых паролей и принуждения пользователей к их смене.

Для выполнения своих функциональных обязанностей по управлению паролями и контролю надежности пользовательских паролей инженеры должны быть предоставлены соответствующие полномочия, позволяющие осуществлять доступ к системным файлам, содержащим пользовательские пароли.

Мониторинг целостности и анализ защищенности

Мониторинг целостности и анализ защищенности ИС включает в себя следующее:

- проверка контрольных сумм и цифровых подписей файлов,
- контроль изменения параметров системного и прикладного ПО,
- проверка прав доступа, связей и размеров файлов и каталогов,
- регистрация фактов добавления и удаления файлов в контролируемых каталогах,
- обнаружение дубликатов идентификаторов пользователей и групп,
- контроль правильности системных конфигурационных файлов.

Активный аудит

Для предупреждения и своевременного выявления попыток несанкционированного входа в систему используются средства активного аудита, которые осуществляют:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования диапазона сетевых портов;
- выявление различных видов локальных и сетевых атак на ресурсы ИС;
- оповещение инженера и другие действия по реагированию на несанкционированные действия в отношении ресурсов ИС со стороны пользователей ИС и внешних нарушителей.

Мониторинг производительности

Косвенной причиной уменьшения производительности системы может являться нарушение безопасности. Мониторинг производительности проводится регулярно в соответствии с планом.

Каждый компонент сети должен иметь контрольно-измерительные средства. Если они отсутствуют, обеспечить бесперебойную работу или даже выяснить причину снижения производительности невозможно.

Если приложение в сети работает недостаточно производительным, то в первую очередь необходимо выявить причину проблемы.

При определении причины недостаточной производительности первоначально нужно выяснить, является ли она постоянной или временной. Например, всегда ли приложение работает непроизводительно или только в период пиковой нагрузки. Если верно первое, то имеет место статическое снижение производительности, если второе – динамическое.

Для того чтобы собрать требуемую информацию, необходимо встретиться с пользователями и выяснить природу возникновения проблемы.

Как только определено, является ли падение производительности статическим или динамическим, можно начинать поиск возможных причин. Динамическое снижение производительности обычно указывает на недостаток ресурсов, к примеру, пропускной способности разделяемой сети или недостаточной производительности процессора хоста, и проблемы, с ними связанные, возникают, как правило, в разделяемых областях инфраструктуры: в сети или на серверах. Сетевые проблемы проявляются в сегментах сети или, что происходит заметно чаще, на промежуточных маршрутизаторах, коммутаторах или шлюзах. Серверные проблемы связаны с нехваткой таких ресурсов, как емкость памяти, мощность процессора или скорость обмена с диском. Динамическое падение производительности происходит в тех случаях, когда потребности в ресурсах превосходят возможности имеющихся ресурсов.

Правильное размещение в сети контрольно-измерительных средств позволит диагностировать и установить причину возникновения динамического снижения производительности, поскольку оно связано с очевидным недостатком ресурсов.

Статическое снижение производительности устранить сложнее, так как очевидных ограничений на ресурсы в этом случае нет. Данные проблемы вызваны в основном недостатками архитектуры. К примеру, сеть не имеет необходимой пропускной способности, клиенты и серверы обладают недостаточной памятью, мощности процессора не хватает, а скорость внутренней шины обмена с диском низка. Неправильное размещение приложений и чрезмерный объем кода графического интерфейса, элементов данных и исполняемых модулей также относятся к изъянам архитектуры.

Зачастую для определения источника статических или архитектурных недостатков необходим сложный анализ, поскольку установленные датчики не всегда правильно указывают причину низкой производительности. В частности, с одной стороны, мониторы производительности, отслеживающие сетевой трафик или загрузку процессора на сервере, не обнаруживают перегрузки, а с другой – приложение не отвечает требованиям пользователей к производительности. Приложение, например, может производить слишком большое число обменов по сети в рамках одной транзакции или чересчур много небольших транзакций, связанных с чтением/записью на диск.

Как только будет определено, в чем состоит проблема, необходимо решить, производить ли модернизацию оборудования или придется изменить архитектуру приложения.

Классификация причин снижения производительности приведена ниже.

Проблемы производительности:

- Динамические:

- Сеть:

- узкие места в маршрутизации;
- недостаточная временная пропускная способность.

- Сервер:

- процессор;
- диск;
- память.

- Статические:

- Приложение:

- код графического интерфейса;
- избыточность элементов данных;
- неоптимальный исполняемый модуль.

- Клиент:

- память;
- диск;
- процессор;
- шина.

- Сервер:

- память;
- шина;
- процессор;
- диск.

- Сеть:

- узкие места в маршрутизации;
- недостаточная пропускная способность.

Синхронизация системных часов

Синхронизация системных часов производится регулярно при помощи соответствующих сетевых программных средств (программных агентов) и является важным условием правильного функционирования системы аутентификации пользователей.

Антивирусные мероприятия

Целесообразно использовать антивирусные программные средства для защиты от вирусов рабочих станций, а также серверов:

- антивирусные сканеры, тестирующие и восстанавливающие файлы и загрузочные секторы дисков, дезактивирующие резидентные части вирусов и тестирующие файлы и системные секторы на наличие неизвестных вирусов;

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

- утилиты для обнаружения и анализа новых вирусов (дисассемблеры, редакторы ОП, трассировщики прерываний и т.п.).

План проведения антивирусных мероприятий состоит из трех основных частей:

1. Предотвращение – мероприятия и правила, позволяющие предотвратить заражение вирусами;
2. Обнаружение – мероприятия, позволяющие определить, что данный выполняемый файл, загрузочная запись или файл данных содержит вирус;
3. Удаление – удаление вируса из зараженной компьютерной системы может потребовать удаления вируса из зараженного файла, удаления файлов или переустановки ОС.

Вероятность заражения вирусами пропорциональна частоте появления новых файлов или приложений на компьютере. Изменения в конфигурации для работы в Интернете, для чтения электронной почты и загрузка файлов из внешних источников – все это увеличивает риск заражения вирусами.

Вирусы обычно появляются в системе из-за действий пользователя (например, установки приложения, получения файла по FTP, чтения электронного письма и т.п.). Поэтому в плане проведения антивирусных мероприятий особое внимание обращено на ограничения по загрузке потенциально зараженных программ и файлов.

Чем выше критичность приложения, обрабатываемого на компьютере, или данных, хранящихся в нем, тем более строгие мероприятия необходимо проводить для предотвращения заражения вирусами.

Все серверы и АРМ пользователей в соответствии с данным критерием (критичность информации) разбиваются на три группы:

1. К группе низкого риска относятся СВТ, на которых обрабатывается и хранится информация, не являющаяся критичной. Кроме того, поток входящих данных минимален либо отсутствует;
2. К группе среднего риска относятся СВТ, на которых обрабатывается и хранится информация, не являющаяся критичной. Поток входящих и исходящих данных средней интенсивности;
3. К группе высокого риска относятся все СВТ, на которых обрабатывается и хранится информация, являющаяся критичной. Кроме того, к данной группе относятся СВТ, обрабатывающие некритичную информацию, но с высоким трафиком входящих и исходящих данных.

Результаты проведенной классификации СВТ оформляются документально и утверждаются директором учреждения.

Низкий риск

Мероприятия по антивирусной защите СВТ с низким риском содержат шаги по доведению до пользователей их обязанностей по регулярной проверке АРМ на наличие вирусов.

Предотвращение

Пользователи должны знать о возможных путях заражения вирусами и о том, как использовать антивирусные средства.

Обнаружение

Антивирусные средства должны использоваться для еженедельной проверки на вирусы. Ведение журналов проверки СВТ на наличие вирусов не является необходимым.

Сотрудники должны информировать инженера о любом обнаруженном вирусе, изменении конфигурации или необычном поведении компьютера или программы. После получения информации об обнаружении вируса инженер должен информировать всех пользователей, имеющих доступ к программам или файлам данных, которые могли быть заражены вирусом, что, возможно, вирус заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы. Пользователи должны сообщить о результатах проверки на вирусы и удаления вируса инженеру.

Инженер обязан доложить о факте заражения вирусом системному администратору.

Удаление

Любая система, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Система не должна подключаться к сети до тех пор, пока инженер не удостоверится в том, что вирус удален.

Средний риск

Мероприятия по антивирусной защите СВТ со средним риском предполагают проведение более частых проверок на вирусы, а также использование антивирусных средств для проверки серверов, связанных с данным СВТ, и электронной почты.

Предотвращение

Программы, установленные на СВТ, должны устанавливаться только инженерами (который проверяет их на вирусы и тестирует).

На файловые серверы должны быть установлены антивирусные программы для ограничения распространения вирусов в сети. Должна производиться ежедневная проверка всех программ и файлов данных на серверах на наличие вирусов. АРМы пользователей должны иметь резидентные антивирусные программы, сконфигурированные так, что все файлы проверяются на вирусы при загрузке на компьютер. Все входящие электронные письма должны проверяться на вирусы. Запрещается запускать программы и открывать файлы с помощью приложений, уязвимых к макровирусам, до проведения проверки этих файлов на вирусы.

С сотрудниками учреждения должны проводиться периодические семинары, содержащие следующую информацию о риске заражения вирусами:

Антивирусные программы могут обнаружить только те вирусы, которые уже были кем-то обнаружены раньше. Постоянно разрабатываются новые, более изощренные вирусы. Антивирусные программы должны регулярно (еженедельно) обновляться для того, чтобы можно было обнаружить самые новые вирусы. Важно сообщать системному администратору о любом необычном поведении компьютера или приложений. Важно сразу же отсоединить компьютер, который заражен или подозревается в заражении, от сети, чтобы уменьшить риск распространения вируса.

Обнаружение

Должны использоваться лицензионные антивирусные программы для ежедневных проверок на вирусы. Антивирусные программы (базы сигнатур) должны обновляться каждую неделю. Все программы или данные, импортируемые в компьютер (с дискет, электронной почты и т.д.), должны перед использованием проверяться на вирусы.

Должны вестись журналы проверки АРМ на наличие вирусов. Данные журналы должны просматриваться инженерами.

Сотрудники должны информировать инженеров об обнаруженных вирусах, изменениях в конфигурации или странном поведении компьютера или приложений.

При получении информации о заражении вирусом инженеры должны информировать всех пользователей, имеющих доступ к программам и файлам данных, которые могли быть заражены вирусом, что вирус, возможно, заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы. Пользователи должны сообщить о результатах проверки на вирусы и удаления вируса инженерам.

Инженеры обязаны доложить о факте заражения вирусом системному администратору.

Удаление

Любая система, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Система не должна подключаться к сети до тех пор, пока инженер не удостоверится в том, что вирус удален.

Высокий риск

Системы с высоким уровнем риска содержат данные и приложения, которые являются критическими для деятельности учреждения. Заражение вирусами может вызвать значительные потери времени, данных и нанести ущерб репутации учреждения. Из-за заражения может пострадать большое число компьютеров. Следует принять все возможные меры для предотвращения заражения вирусами.

Предотвращение

Установка ПО на серверы и АРМ пользователей производится непосредственно инженерами. К эксплуатации в ИС допускается только лицензионное ПО, приобретенное непосредственно у производителя либо его официального представителя. Перед установкой ПО должно пройти тестовые испытания на стенде. Конфигурация ПО на АРМ пользователей должна проверяться еженедельно на предмет выявления программ, самостоятельно установленных пользователями.

С целью ограничения риска заражения ПО должно устанавливаться только с разрешенных внутренних серверов либо с лицензионных носителей. Запрещено загружать ПО из Интернета.

На серверах должны быть установлены антивирусные средства для предотвращения заражения и распространения вирусов в сети. Должна производиться ежедневная проверка всех программ и файлов данных на серверах на наличие вирусов.

На АРМ пользователей должны устанавливаться резидентные антивирусные средства, сконфигурированные так, что все файлы проверяются на вирусы при загрузке на компьютер. Запрещается запускать программы и открывать файлы с

помощью приложений, уязвимых к макровирусам, до проведения проверки этих файлов на вирусы.

Все входящие письма и файлы, полученные из сети, должны проверяться на вирусы при получении. Рекомендуется использование антивирусных средств, установленных на межсетевых экранах. Данные средства способны выполнять «на лету» проверку всего входящего и исходящего трафика сегмента сети.

С сотрудниками учреждения должны проводиться инструктажи, содержащие следующую информацию о риске заражения вирусами.

Антивирусные программы могут обнаружить только те вирусы, которые уже были кем-то обнаружены ранее. Постоянно разрабатываются новые, более изощренные вирусы. Антивирусные программы должны регулярно (ежемесячно) обновляться для того, чтобы можно было обнаружить самые новые вирусы. Важно сообщать инженеру о любом необычном поведении компьютера или приложений. Важно сразу же отсоединить компьютер, который заражен или подозревается в заражении, от сети, чтобы уменьшить риск распространения вируса.

Невыполнение данных мероприятий должно вести к наказанию сотрудника согласно правилам, принятым в учреждении.

Обнаружение

Должны использоваться лицензионные антивирусные программы для ежедневных проверок на вирусы. Антивирусные программы (базы сигнатур) должны обновляться каждую неделю. Все данные, импортируемые в компьютер (с дискет, электронной почты и т.д.), должны перед использованием проверяться на вирусы.

Должны вестись журналы проверки АРМ пользователей на наличие вирусов. Данные журналы должны просматриваться и анализироваться инженерами.

Проверка серверов должна производиться каждый день в обязательном порядке. Результаты проверок должны протоколироваться, автоматически собираться и анализироваться инженерами.

Сотрудники обязаны информировать инженера об обнаруженных вирусах, изменениях в конфигурации или странном поведении компьютера или приложений.

При получении информации о заражении вирусом инженер должен информировать всех пользователей, имеющих доступ к программам и файлам данных, которые могли быть заражены вирусом, что вирус, возможно, заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы.

Инженеры обязаны доложить о факте заражения вирусом системному администратору.

Удаление

Любая система, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Система не должна подключаться к сети до тех пор, пока инженер не удостоверится в удалении вируса. Для удаления вируса должны использоваться только лицензионные программы, приобретенные непосредственно у разработчика либо его официального представителя.

Если используемые антивирусные средства не могут удалить вирус либо предупреждают о некорректном восстановлении поврежденной информации, то необходимо обратиться по телефону либо электронной почте к фирме-

изготовителю с целью получения обновленной версии программы-антивируса. Также возможен вариант вызова специалиста из фирмы, оказывающей экстренную помощь при заражении компьютерными вирусами.

В крайнем случае допускается уничтожение вируса путем форматирования носителя информации (предварительно загрузившись с «чистой» операционной системы), с дальнейшим восстановлением программного обеспечения и данных с резервных копий.

После восстановления СВТ должно быть повторно проверено на наличие вирусов.

Каждый случай заражения сервера или АРМ пользователя должен тщательным образом анализироваться. На основе выводов должны быть сформулированы предложения и внесены изменения в технологическую цепочку обработки критичной информации.

Пользователи ИС, в результате действий которых произошло искажение (уничтожение) критичной информации, подлежат наказанию в соответствии с правилами, принятыми в учреждении.

Мониторинг внешних источников информации

Мониторинг внешних источников информации производится системным администратором регулярно в соответствии с планом и включает в себя получение информации об уязвимостях используемых ОС и МЭ, выпуске пакетов программных коррекций и других вопросах безопасности.

Аудит безопасности

Аудит безопасности производится системным администратором регулярно, а также в ситуациях, требующих проведения расследования инцидента, связанного с нарушением информационной безопасности ИС.

Обзоры безопасности

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния ИС тому уровню защищенности, который удовлетворяет требованиям политики безопасности. Выделяют три уровня защищенности: низкий, средний и высокий. Для каждого из этих уровней описывается состояние системы в терминах неизменности системной конфигурации и целостности системных файлов (таблиц), системных программ, СУБД, приложений, сетевых сервисов и системных устройств. Обзоры безопасности проводятся с целью выявления всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку проверки (например, шаблоны значений параметров настройки ОС). Для проведения проверок и составления отчетов используются автоматизированные программные средства инженера и программиста, работающие либо в интерактивном, либо в фоновом режиме. Обзоры безопасности, как минимум, должны включать следующие пункты:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских системных окружений;

- выявление троянских программ при помощи антивирусных средств и сетевых сканеров;

- проверка содержимого конфигурационных файлов ОС на соответствие спискам проверки;

- выявление изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверка прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

- проверка правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

- проверка корректности конфигурации системных устройств и активного сетевого оборудования (мостов, маршрутизаторов, концентраторов и межсетевых экранов).

Активное тестирование системы защиты

Активное тестирование – тестирование механизмов контроля доступа путем осуществления попыток проникновения в систему и других видов атак (с помощью автоматического инструментария или вручную).

Пассивное тестирование системы защиты

Пассивное тестирование механизмов контроля доступа, в отличие от активного, осуществляется путем анализа конфигурационных файлов ОС, а также МЭ и прочих СЗИ НСД. Информация об известных уязвимостях извлекается из документации и внешних источников информации. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний, т.е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Контроль внесения изменений в системное программное обеспечение и установки программных коррекций

Внесение изменений производится с уведомлением каждого, кого касается предлагаемое изменение. Контроль внесения изменений осуществляется периодическими проверками состава и конфигурации СВТ и сравнения его с данными, указанными в паспорте на СВТ (ИС).

Планирование конфигурации подсистемы аудита безопасности

Планирование конфигурации подсистемы аудита безопасности включает в себя следующие шаги:

- *Спланировать хранение журналов аудита:*

1. Определить для каждой контролируемой системы классы событий, которые будут регистрироваться.
2. Определить, какие события к какому классу относятся.
3. Определить, какое количество информации аудита необходимо генерировать для каждой контролируемой системы. Найти компромисс между требованиями обеспечения безопасности и количеством доступного для аудита дискового пространства.
4. Определить, какие компьютеры будут выполнять роль серверов аудита и какие будут клиентами для этих серверов.
5. Определить имена и расположение файловых систем для аудита.
6. Спланировать использование файловых систем на серверах аудита.

- *Определить, какие действия и для каких пользователей будут отслеживаться:*

7. Определить, для каких классов событий желательно осуществлять аудит.
8. Определить, какие пользователи должны быть подвергнуты более тщательному наблюдению.
9. Определить, какое минимальное количество дискового пространства должно оставаться на диске, прежде чем посылать предупреждение администратору аудита.
10. Определить конфигурацию подсистемы аудита безопасности.
11. Определить стратегию аудита - стратегия аудита определяет различные детали, связанные с аудитом, например, следует ли включать в записи аудита их порядковые номера или данные о группе пользователя, а также следует ли регистрировать информацию об окружении и аргументах командной строки вызываемых программ.

Анализ журналов аудита

Анализ больших объемов информации осуществляется с использованием специализированного программного инструментария.

В качестве исходных данных для анализа используется информация из следующих источников:

Внешний аудит безопасности

В отличие от внутреннего аудита, внешний аудит безопасности производится независимыми экспертами, не имеющими отношения к администрированию системы.

Внешний аудит безопасности входит в состав комплекса работ по аудиту ИС наряду с вопросами анализа надежности, производительности, разрешения проблемных ситуаций и т. д.

Целями проведения аудита безопасности являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- выработка рекомендаций и требований по обеспечению безопасности ИС.

Использование криптографических методов защиты информации от НСД

Для обеспечения конфиденциальности и целостности критичной информации при передаче ее по каналам связи, проходящим вне контролируемой зоны, а также при хранении информации на магнитных носителях, необходимо использовать криптографические методы защиты информации. Программные и/или аппаратные средства криптографической защиты информации выбираются исходя из необходимости обеспечить определенный уровень защиты в соответствии с требованиями политики информационной безопасности. В целом, должно быть предусмотрено:

- использование систем шифрования с открытыми и закрытыми ключами для обеспечения конфиденциальности электронных документов;
- использование средств электронной подписи для подтверждения авторства и контроля целостности электронных документов.

Выявление попыток НСД

Анализ инцидента программистом

Если программист подозревает или получил сообщение о том, что вверенная ему система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки НСД;
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД (получение прибыли, саботаж, шпионаж, любопытство и т.д.).

Для выявления нарушений безопасности, на серверах ЛВС, которые могли оказаться скомпрометированными в результате осуществления попытки НСД, системному администратору совместно с инженерами и программистом необходимо провести следующие технические мероприятия:

Выявление активных пользователей

Необходимо установить, какие пользователи в настоящее время работают в системе, способ входа пользователей в систему, на каких терминалах и какие процессы они выполняют.

Выявить подозрительную активность пользователей:

- проверить допустимость имен пользователей;
- проверить, что никто из пользователей не работает в системе необычно долго;
- проверить, что все пользователи вошли в систему со своих рабочих мест (терминалов, рабочих станций и т.п.);
- проверить, что никто из пользователей не выполняет подозрительных программ и задач, не относящихся к его области деятельности.

Выявление подозрительных процессов

Необходимо установить, какие процессы в настоящее время активны в системе, подвергающейся атаке.

Выявить подозрительные процессы:

- процессы, активные в течение промежутков времени более длительных, чем допустимые для них;
- необычные времена начала выполнения задач (такие как 3.00);
- необычные имена процессов;
- процессы, занимающие высокий процент рабочего времени ЦП;
- процессы, не имеющие управляющего терминала, которые выполняют необычные программы.

Проверка конфигурации сетевых адаптеров

Необходимо проверить конфигурацию сетевых адаптеров с целью выявления установленных на скомпрометированных системах программ, используемых для просмотра и анализа сетевого трафика:

- проверить, не находится ли сетевой адаптер в режиме приема всех пакетов своего сетевого сегмента;
- проверить, не появились ли в системе новые файлы;
- проверить, не запущен ли процесс, потребляющий очень высокий процент процессорного времени.

Проверка системы на наличие в ней файлов или других следов, оставленных злоумышленником

Для обнаружения в системе оставленных злоумышленником следов в виде файлов, вирусов, троянских программ, а также изменений системной конфигурации, необходимо провести антивирусное сканирование и проверку целостности файловых систем серверов ЛВС с использованием соответствующих антивирусных средств и средств контроля целостности.

Автоматическое выявление нарушений безопасности

Автоматическое выявление нарушений безопасности производится с помощью специализированных программных средств и методов для осуществления непрерывного мониторинга действий пользователей в реальном времени с целью обнаружения подозрительной активности.

Можно выделить следующие программные средства и методы:

- использование экспертных систем, базирующихся на установлении рабочих профилей отдельных пользователей (вид и характер работы, особенности работы, скорость работы с клавиатурой и т.п.);
- использование экспертных систем, базирующихся на определении правил для выявления подозрительных действий при анализе журналов аудита;
- использование экспертных систем, базирующихся на знании известных уязвимостей системы и сценариев атак;
- использование ловушек (ложные пользователи, пароли, о попытках использования которых немедленно сообщается администратору системы и т.п.).

Реагирование на нарушения информационной безопасности

Первоначальные действия

1. Известить директора учреждения.
2. Определить круг лиц, принимающих участие в предварительном анализе инцидента.

Анализ инцидента

Оценка серьезности инцидента

1. Оценить уровень серьезности инцидента и определить степень риска:
 - Уровень 1 – критическое событие. Попытка НСД продолжается и/или серьезная уязвимость в механизмах безопасности системы (или сети) была обнаружена и использована для НСД.
 - Уровень 2 – событие, требующее немедленного вмешательства. Вероятность НСД, вызванного уязвимостью, очень высока, но НСД мог еще не произойти.
 - Уровень 3 – проблема с компьютером или с сетью, требующая немедленного внимания.
 - Уровень 4 – некритическое событие, которое должно быть задокументировано для обеспечения последующих ссылок на него.
 - Уровень 5 – только информация, требующая немного либо вообще не требующая внимания.
2. Оценить масштаб инцидента – безопасность каких ресурсов нарушена.
3. Оценить причиненный ущерб.

Составление базового профиля нарушителя

Базовый профиль нарушителя включает следующие сведения:

- Кто является нарушителем (сотрудник учреждения либо внешний нарушитель);
- Какова его мотивация (саботаж, шпионаж, любопытство, самоутверждение или получение прибыли);
- Каковы возможности нарушителя.

Опрос персонала

Необходимо опросить персонал с целью выяснения подробностей осуществления НСД к информации.

Взаимодействие с консультантами и поставщиками ПО

В случае необходимости следует связаться с независимыми консультантами или поставщиками ПО для получения помощи в диагностировании нарушений безопасности.

Определение состава мероприятий по реагированию на нарушение безопасности

На основе произведенного анализа инцидента системный администратор принимает решение о целесообразности дальнейших действий. Если серьезность инцидента соответствует Уровню 5, то никаких действий предпринимать не требуется. Для Уровня 4 необходимо только задокументировать инцидент в соответствующем журнале. В случае, если серьезность инцидента соответствует Уровням 1 – 3, возможны две стратегии реагирования на нарушение безопасности. Первая стратегия заключается в том, чтобы немедленно прервать попытку НСД, защитить ИС от несанкционированных действий, ликвидировать нарушения и позволить пользователям продолжать работу с ИС. Вторая заключается в том, чтобы позволить нарушителю продолжать попытку НСД с целью осуществления мониторинга его действий.

Стратегия немедленной защиты и восстановления выбирается при следующих условиях:

- если ресурсы ИС недостаточно хорошо защищены от нарушителя;
- если действия нарушителя могут привести к большому финансовому риску и нанести серьезный ущерб;
- если преследование нарушителя невыгодно с финансовой точки зрения, либо отсутствует такая возможность, либо желание;
- если существует значительный риск для пользователей ИС;

Стратегия наблюдения за нарушителем и его преследования выбирается при следующих условиях:

- ресурсы ИС адекватно защищены;
- последствия возможных последующих попыток НСД перевешивают риск, которому подвергается ИС в настоящий момент;

- попытка НСД является продолжением предыдущих попыток, уже имевших место ранее;
- отказ от преследования нарушителя может спровоцировать новые попытки НСД;
- доступ нарушителя к ресурсам ИС находится под контролем;
- средства мониторинга в состоянии осуществлять достаточно полное протоколирование действий нарушителя для того, чтобы собрать необходимые доказательства для принятия мер по привлечению нарушителя к ответственности;
- системным администратором достаточно хорошо подготовлены в плане знания ОС, системных утилит, СУБД и прикладных систем, чтобы осуществлять отслеживание действий нарушителя.

Осуществление мониторинга действий нарушителя безопасности

Мониторинг действий нарушителя должен осуществляться незаметно для него. Все действия нарушителя должны регистрироваться в журнале попыток НСД с тем, чтобы собрать достаточное количество доказательств для привлечения его к ответственности.

После того, как с помощью мониторинга попытки НСД будет собрано достаточное количество доказательств для привлечения нарушителя к ответственности, нужно прервать попытку НСД, оценить причиненный ущерб и, в случае необходимости, перейти к ликвидации последствий НСД, либо сразу приступить к принятию мер по привлечению нарушителя к ответственности.

Немедленное реагирование на нарушение безопасности

Стратегия немедленного реагирования требует принятия решения относительно целесообразности временной остановки работы отдельных компонентов ИС с целью прекращения несанкционированных действий со стороны нарушителя. После того, как попытка НСД остановлена, следует переходить к ликвидации последствий инцидента.

Недостатком данного подхода является его вынужденность и связанная с этим недостаточная гибкость. Нарушитель узнает о том, что он обнаружен, и предпримет ответные действия с целью скрыть следы своей деятельности. Нарушитель также может изменить стратегию атаки на ресурсы ИС или продолжить попытку НСД к другим ресурсам, ранее не затронутым инцидентом.

Ликвидация последствий НСД

Первоначальные действия

1. Установить приоритет восстановительных работ и распределить обязанности.
2. В случае необходимости объявить об инциденте пользователям ИС.
Решение относительно целесообразности уведомления об инциденте пользователей ИС принимается на основании результатов анализа инцидента,

исходя из политических и практических соображений, а также в зависимости от уровня серьезности инцидента. Объявление о факте удавшейся попытки НСД подрывает престиж учреждения и вызывает у клиентов недоверие к ней. С другой стороны, в некоторых случаях полная ликвидация последствий НСД требует участия пользователей ИС.

В результате попытки НСД пользовательские пароли и файлы могут оказаться скомпрометированными, поэтому пользователи должны сменить свои пароли и проверить целостность своих личных файлов и каталогов. При этом им следует обратить внимание на появление новых файлов (каталогов), исчезновение старых, на изменение контрольных сумм и размеров бинарных файлов, а также на изменение содержимого текстовых файлов.

Проведение антивирусных мероприятий

Если обнаружен компьютерный вирус, необходимо провести централизованное сканирование файловых систем на серверах ЛВС и рабочих местах пользователей в соответствии с планом проведения антивирусных мероприятий.

Восстановление данных с резервных копий

Восстановление данных, целостность которых была нарушена в результате осуществления несанкционированных действий, на серверах ЛВС осуществляется в соответствии с процедурой резервного копирования и восстановления данных.

Смена паролей на скомпрометированных системах

Сменить все пароли на скомпрометированных системах и известить об этом пользователей.

Анализ выявленных уязвимостей

При анализе уязвимости, ставшей причиной успешного осуществления НСД к ресурсам ИС, рассматриваются следующие вопросы:

1. Легко ли воспроизвести данную уязвимость;
2. Присутствует ли она в различных версиях ПО;
3. Предоставляет ли уязвимость привилегированный доступ;
4. Может ли уязвимость использоваться для получения привилегированного доступа в будущем;
5. Какие компоненты ИС подвержены этой уязвимости.

Ликвидация уязвимости

Ликвидация уязвимостей ПО обычно осуществляется путем установки соответствующих пакетов программных коррекций либо путем перехода на другую версию ПО.

Установка пакетов программных коррекций, внесение изменений в ПО или в конфигурацию ИС осуществляются в соответствии с процедурой внесения изменений в ПО.

Воспроизведение картины событий и документирование нарушения безопасности

Необходимо воспроизвести картину осуществления НСД к ресурсам ИС и задокументировать последовательность событий.

Следует также задокументировать причину инцидента, уязвимости, которые были использованы для осуществления НСД, и последовательность мероприятий по восстановлению целостности данных и работоспособности ИС в журнале регистрации фактов нарушений информационной безопасности.

Решение этой задачи может оказаться невозможным без показаний самого нарушителя безопасности. Также может потребоваться помощь пользователей и персонала ИС.

Завершающие мероприятия

1. Подготовить информацию для принятия мер, связанных с привлечением нарушителя безопасности к ответственности.
2. Провести собрание рабочей группы, принимавшей участие в ликвидации последствий НСД, с целью обсуждения и оценки проделанной работы.
3. При необходимости внести изменения и/или дополнения в настоящее План.

Рассмотрено
Советом Учреждения
Протокол № 22
«24» 05 2022 г.

В дело № 01-14
«24» 05 20 22 г.

Перечень сокращений

БД - База данных

ОС - Операционная система

ПИБ - Подсистема информационной безопасности

ИС - Информационная система

ПО - Программное обеспечение

СВТ - Средства вычислительной техники

СЗИ - Средства защиты информации

НСД - Несанкционированный доступ