УДК 004.056

Анализ технических мероприятий по обеспечению информационной безопасности компьютерной сети с операционной системой Astra Linux

К.В. Новиковский✉

Воронежский институт высоких технологий, Воронеж, Россия

В статье рассмотрены и проанализированы технические мероприятия по обеспечению информационной безопасности компьютерной сети с операционной системой Astra Linux. Составлена модель предполагаемого нарушителя, а также сформулированы требования, выполнение которых является обязательным для поддержания информационной безопасности компьютерной сети.

Ключевые слова: компьютерная сеть, ОС Astra Linux, информационная безопасность.

Analysis of technical measures to ensure information security of computer network with operating system Astra Linux

K.V. Novikovskiy✉

Voronezh Institute of High Technologies, Voronezh, Russia

The article considers and analyses technical measures to ensure information security of a computer network with the operating system Astra Linux. The model of the supposed intruder is made, and also the requirements, fulfilment of which is obligatory for maintenance of information security of a computer network, are formulated.

Keywords: computer network, Astra Linux OS, information security.

Введение

Компьютерная сеть является основой современной организации, так как обеспечивает единое функционирование всех подразделений. В силу своей критической важности необходимость обеспечения информационной безопасности компьютерной сети является первостепенной задачей. Цель написания данной статьи заключается в анализе технических мероприятий по обеспечению информационной безопасности компьютерной сети. Практическая ценность данного анализа заключается в выявлении уязвимостей и рассмотрении защитных мер, что позволяет повысить уровень информационной безопасности.

Структурная схема компьютерной сети

При проведении анализа технических мероприятий по обеспечению информационной безопасности компьютерной сети необходимо рассмотреть программно-технический комплекс этой сети.

Рассмотрим элементы, которые входят в программно-технический комплекс: сервер, компьютеры, активное сетевое оборудование, каналы передачи данных, программное обеспечение, оборудование периферии.

Сервер – это электронная вычислительная машина с функцией управления, на которую поступает вся информация от устройств, расположенных на территории

организации. На сервере производится аналитика информации и формируется журнал событий, происходящих во всех системах организации.

Компьютер – это электронное устройство, предназначенное для обработки, хранения и передачи данных. Компьютеры объединены в локальную сеть, что позволяет производить обмен данными между различными системами, что важно для функционирования всей организации.

Активное сетевое оборудование состоит из управляемых коммутаторов, расположенных по всей территории организации. Именно данное оборудование обеспечивает маршрутизацию и коммутацию потоков данных. Каналы передачи данных представляют собой оборудование, которое находится на территории организации и объединено в локальную вычислительную сеть. Передача информации от технологических устройств до сетевого оборудования осуществляется по кабелю типа «витая пара». Передача информации между активным сетевым оборудованием, расположенным на значительном расстоянии, осуществляется по волоконно-оптическим линиям связи.

К периферийному оборудованию относятся устройства, контролирующие технологические процессы.

Программное обеспечение, устанавливаемое на серверы, является специально разработанным и включает в себя механизмы мониторинга сетевой активности, обнаружения вторжений, антивирусную защиту и брандмауэры.

Модель нарушителя, угрозы информационной безопасности и элементы, к которым необходимо применять меры информационной безопасности

В рамках анализа технических мероприятий по обеспечению информационной безопасности компьютерной сети можно составить модель нарушителя и определить угрозы информационной безопасности.

Нарушителем информационной безопасности является любой пользователь, который своими действиями умышленно или неумышленно нарушает правила и политику безопасности информационной системы. Нарушителей можно разделить на две категории: внешние и внутренние. Внешние нарушители – это отдельные лица или организации, не связанные с внутренними процессами организации. Вредоносное воздействие направлено через внешние уязвимости информационной системы. Внутренние нарушители – это сотрудники организации, имеющие прямой доступ к информационной системе и данным. Например, сотрудник отдела продаж, который не обладает необходимыми техническими знаниями для умышленного вредоносного воздействия, может случайно отправить электронное письмо с конфиденциальной информацией не тому адресату, что приведёт к утечке данных.

Однако внутренние нарушители могут действовать и осознанно. Например, сотрудник отдела информационной безопасности, обладающий необходимыми техническими знаниями и имеющий доступ к конфиденциальной информации компании, может передать часть сведений злоумышленнику. В случае неумышленного воздействия цель как таковая отсутствует, а в случае умышленного воздействия она может варьироваться от личной выгоды до нанесения ущерба организации в рамках индивидуальных или конкурентных интересов.

Учитывая модель нарушителя, можно выделить некоторые типовые угрозы, такие как получение доступа к служебной информации путём перехвата файлов в момент передачи, внедрение вредоносного программного обеспечения для повреждения файловой архитектуры операционной системы, подмена подлинной

электронной документации (например, подмена письма или распоряжения с целью получения учётных данных сотрудников).

Анализируя вышеописанное, можно определить элементы, к которым необходимо применять меры информационной безопасности:

– информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, информация о конфигурации систем и сетей, данные телеметрии и др.);

– программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства)) [1];

– программные средства (в том числе системное и прикладное программное обеспечение, включая серверы приложений, системы управления базами данных);

– машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;

– телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);

– средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);

– учётные записи привилегированных и непривилегированных пользователей систем и сетей, а также пользовательские интерфейсы.

Требования, установленные к информационной безопасности компьютерной сети

Учитывая модель нарушителя, угрозы и элементы, к которым необходимо применять меры информационной безопасности можно сформулировать специальные требования по обработке конфиденциальной информации и информационной безопасности:

– централизованное создание, активация, модификация, пересмотр (с установленной периодичностью), отключение и удаление учётных записей;

– централизованное хранение идентификационных данных пользователей;

– автоматизация процессов управления привилегиями пользователей;

– управление доступом в локальную вычислительную сеть (сетевые сегменты).

Анализ решений по обеспечению информационной безопасности

Учитывая модель нарушителя и требования Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27 июля 2006 г., а также Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», можно сделать вывод о том, что технические мероприятия по обеспечению информационной безопасности осуществляются с целью обеспечения целостности, доступности и конфиденциальности обрабатываемой информации и предусматривают формирование ряда подсистем обеспечения информационной безопасности. Рассмотрим и проанализируем данные подсистемы и их функции.

Подсистема управления доступом выполняет настройку разграничения доступа на всех серверах и компьютерах, а также даёт возможность авторизованным пользователям получать доступ к информации, необходимой для выполнения служебных обязанностей.

Подсистема регистрации и учёта выполняет настройку встроенных средств регистрации и учёта прикладного программного обеспечения на сервере, а также настройку встроенных механизмов регистрации и учёта антивирусного программного обеспечения. Данная подсистема необходима для обеспечения мониторинга событий, связанных с обеспечением безопасности информации. Далее рассмотрим некоторые параметры, регистрация и учёт которых реализуются в рамках данной подсистемы для минимизации рисков несанкционированного доступа, улучшения управления правами пользователей и повышения оперативности реакции на инциденты:

– аутентификация пользователей и контроль завершённости сеанса осуществляется посредством регистрации даты и времени каждого входа в систему и времени выхода и завершения сеанса, что позволяет вести статистику по использованию сети;

– доступ к ресурсам осуществляется путём записи информации о каждом доступе к ресурсам, включая имя пользователя, время доступа, тип доступа (чтение, запись, удаление), имя ресурса и результат доступа (успешный или неуспешный). Эта информация позволяет отслеживать несанкционированный доступ и анализировать использование ресурсов;

– системные события и сообщения, фиксирующие все уведомления или сообщения, возникающие в операционной среде регистрируются в журнале событий. Журнал событий содержит информацию о времени события, типе события (ошибка, предупреждение, информация), источнике события и подробное описание произошедшего. Это позволяет отслеживать внештатные ситуации, диагностировать проблемы и анализировать активность системы;

– контроль доступа к ресурсам осуществляется посредством записи действий каждого пользователя сети, а именно к каким файлам, директориям или приложениям обращался пользователь. В итоге формируется отчёт на каждого пользователя сети, в котором содержится дата и время обращения к определённому ресурсу, а также тип доступа, а именно: чтение, запись, модификация или удаление данных. Данная функция позволяет управлять доступом к конфиденциальной информации, а также уменьшить риски несоблюдения установленных ограничений.

Подсистема обеспечения целостности. Функция данной подсистемы заключается в наблюдении за программными средствами с целью обнаружения несанкционированных изменений и ведения журнала о количестве изменений, внесённых в программные средства. Далее рассмотрим некоторые параметры текущей подсистемы, которые позволяют определить факт корректной работы программных средств:

– контроль целостности файлов реализуется через несколько основных этапов. Основными элементами являются алгоритмы хэширования, такие как MD5 и SHA-256, которые используются для проверки целостности файлов и директорий на предмет внесённых изменений. Существенным элементом в этом процессе является фиксация даты и времени последнего изменения файла, что обеспечивает возможность мониторинга временных меток изменений. Кроме того, контроль целостности каждого отдельного файла в системе осуществляется с помощью хэш-сумм, которые служат идентификаторами файлов и позволяют эффективно проверять их целостность;

– тестирования и валидации основываются на регулярной проверке программных средств защиты информации на предмет выявления уязвимостей. Важным этапом данного параметра является валидация всех изменений в программном обеспечении, которая происходит перед его развёртыванием в сети, что обеспечивает

дополнительный уровень безопасности и минимизирует риски негативного воздействия на систему.

Для обеспечения антивирусной защиты информационных ресурсов необходимо предусматривать антивирусное программное обеспечение с возможностью управления защитой всех компьютеров и устройств в сети через централизованную панель администрирования.

Подсистема обеспечения непрерывности функционирования средств защиты информации регулярно производит обновление программного обеспечения и средств антивирусной защиты, а администратором локально-вычислительной сети производится резервное копирование и восстановление конфигурационных файлов средств обеспечения информационной безопасности с использованием встроенных средств [2].

Программное обеспечение, устанавливаемое на серверы и компьютеры определяется требованиями нормативных актов, которые регулируют способы обработки информации, в частности, Федеральным законом Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г. Учитывая данный правовой документ, для обеспечения информационной безопасности можно использовать операционную систему Astra Linux.

Далее рассмотрим некоторые особенности операционной системы Astra Linux, которые важны для информационной безопасности. Операционная система Astra Linux построена на концепции макроядра, которое составляет основу системы. Без ядра операционная система является полностью неработоспособной и не сможет выполнить ни одну из своих функций.

Макроядерная архитектура обеспечивает высокую производительность благодаря выполнению большинства функций в одном ядре, что способствует быстрой обработке запросов. Упрощённая разработка и поддержка системы позволяют эффективно управлять обновлениями безопасности и исправлениями уязвимостей. Целостность системы достигается за счёт того, что все компоненты функционируют в одном адресном пространстве, что снижает вероятность возникновения уязвимостей. Встроенные механизмы безопасности, такие как управление доступом, регистрация и учёт, протоколирование и проверка целостности, способствуют предотвращению несанкционированного доступа. Упрощённая обработка вызовов между модулями увеличивает скорость взаимодействия. Широкая поддержка приложений формирует надёжную экосистему для пользователей, что дополнительно усиливает безопасность системы [3].

Далее рассмотрим механизм управления доступом. Каждому сотруднику, в должностные обязанности которого входит обслуживание или работа в компьютерной сети, выделяется уникальный логин и пароль. Когда пользователь вводит свой логин и пароль, он проходит процедуры аутентификации, подтверждая свою личность. После процесса аутентификации ключевым элементом становится идентификация пользователя, и для этого система использует уникальный идентификатор пользователя (User ID, UID). Этот числовой идентификатор при регистрации в системе присваивается каждому пользователю, а затем определяется в группы. Каждый пользователь может принадлежать к нескольким группам, и всем группам присвоен уникальный идентификатор группы (Group Identifier, GID) [4].

На основе UID и GID система определяет, к каким файлам и ресурсам пользователь имеет доступ. В операционной системе Astra Linux предусмотрено три типа пользователей:

1. Первый тип – это владелец файла (owner). Данный пользователь создал файл и имеет множество прав на него, в том числе и редактирование. Примером может являться системный администратор.

2. Второй тип – это группа (group), объединение пользователей, которых связывает доступ к общему файлу. Права доступа, установленные для данной группы, определяют действия, которые они могут совершать с файлами. Примером являются сотрудники организации.

3. Третий тип – это другие пользователи (others). Эти пользователи не принадлежат к группам и не являются владельцами файлов. Примером могут быть сотрудники подрядных организаций, которые проводят работы в сети.

Для всех файлов установлены права доступа. В Astra Linux эти права обозначаются в виде букв:

– права чтения (r);
– права редактирования (w).

Например, права доступа могут быть обозначены следующим образом: (rw-r—r). Эта запись означает, что владелец файла имеет права на редактирование файла, а члены группы обладают только правами чтения.

Рассмотрим работу механизма управления доступом. Когда пользователь пытается открыть файл, система проводит проверку, чтобы определить, кто запрашивает доступ, используя UID, а затем определяется, к какой группе относится данный пользователь, используя GID. Далее система анализирует все исходные данные и отправляет пользователю решение о предоставлении или отказе в доступе к запрашиваемому ресурсу.

Теперь рассмотрим механизм регистрации и учёта, протоколирования в ОС Astra Linux. Данный алгоритм в операционной системе осуществляется по команде syslog или журналу. В данный журнал записываются события аутентификации, системные ошибки и предупреждения, а также обращения к критическим файлам [5]. Под событиями аутентификации подразумевается количество успешных и безуспешных входов в систему. Системные ошибки – это ошибки, которые возникают при выполнении системных процессов, а предупреждения могут означать, например, недостаточный объём памяти. Критическими файлами являются файлы, изменение которых может повлиять на безопасность и работоспособность сети. Такими файлами являются, например, /etc/passwd и /etc/shadow – эти файлы содержат информацию о пользователе и пароли, которые он использует в работе, а также файлы конфигурации сервисов, таких как SSH. Основная запись в журнале событий содержит в себе информацию о дате, когда произошло событие, его типе и приоритете события. Все файлы журналов хранятся в каталоге /var/log и его подкаталогах.

В файлах журналов сообщения записываются вместе со всеми параметрами в текстовом виде, что упрощает процесс поиска и анализа событий. Для решения проблем, связанных с размером журнала и поиском информации о недавно произошедших событиях в системе необходимо установить периодичность форматирования событий. Протоколирование работы пользователей в ОС Astra Linux и информация о сеансах работы пользователей записываются в несколько файлов в каталоге. Информация в этих файлах хранится в двоичном коде, а не в текстовом виде.

Механизм контроля целостности. Для проверки целостности в Linux предусмотрена утилита fsck. Эта утилита является базовым компонентом дистрибутива ОС Astra Linux. Алгоритм работы данной утилиты заключается в поиске подлогов и изменений исходных файлов, когда они были заменены инсталлятором или вредоносным программным обеспечением.

Частью контроля целостности файлов является резервное копирование и восстановление удалённых файлов. В операционной системе Astra Linux за данную функцию ответственны утилиты tar, restore и dump. Утилита tar позволяет производить восстановление удалённых или повреждённых файлов, а также выполнять резервное копирование файлов и каталогов на внешние запоминающие устройства. Утилита dump выполняет практически те же функции, что и tar, но она предназначена в основном для работы с файловыми системами и дополняет процедуру restore, которая предназначена для восстановления файлов из резервной копии, созданной процедурой dump.

Для автоматизации процедуры резервного копирования используется команда cron, которая управляет выполнением запланированных событий. Мероприятия по созданию резервных копий проводятся администратором локальной вычислительной сети с использованием внешних носителей информации.

Заключение

В заключение можно сделать вывод о том, что технические мероприятия по обеспечению информационной безопасности благодаря своим алгоритмам работы обеспечивают предотвращение и (или) снижение ущерба от инцидентов информационный безопасности и стабильность основных производственных процессов, а операционная система Astra Linux благодаря своим безопасным алгоритмам работы собирает все подсистемы в единую систему информационной безопасности.

СПИСОК ИСТОЧНИКОВ

1. Михайлов К.М. Алгоритм разработки мероприятий по нейтрализации угроз информационной безопасности предприятия / К.М. Михайлов // Актуальные исследования. – 2024. – № 25-2 (207). – С. 64-68.

2. Мельников В.П. Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности «Информационные системы и технологии» / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – 2-е изд., стер. – Москва: Academia, 2007. – 336 с.

3. Окороков В.А. Защищенные операционные системы / В.А. Окороков // Вестник УрФО. Безопасность в информационной сфере. – 2015. – № 1 (15). – С. 33-37.

4. Шаповалов С.Л. Контроль доступа в ОС ASTRA LINUX / С.Л. Шаповалов, И.А. Сомов, Г.В. Сконодобов // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. – 2018. – № 1 (9). – С. 212-215.

5. Любчич В.А. Модель угроз безопасности информации / В.А. Любчич // Студент: наука, профессия, жизнь: Материалы X всероссийской студенческой научной конференции с международным участием: в 5-ти частях. – Омск: Омский государственный университет путей сообщения, 2023. – Ч. 3. – С. 103-109.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Новиковский Константин Викторович, студент, Воронежский институт высоких технологий, Воронеж, Россия.
e-mail: kostya0361@yandex.ru