Пустовой Андрей Игоревич

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Распределенные автоматизированные системы

Разработка и реализация мер по обеспечению информационной безопасности

Аннотация. В статье рассматриваются предложения по улучшению мер информационной безопасности в информационно – вычислительной системе учреждений.

Ключевые слова: информационная безопасность, системы единого управления, оптимизация ресурсов, автоматизированное управление.

Защита информации на предприятиях должна осуществляться непрерывно и охватывать все организационные и производственные процессы. Для реализации постоянного процесса защиты информации необходимо применение системного подхода, а также создание условий и механизмов защиты информации. Обеспечение в полном объеме на сегодняшний день мер по обеспечению информационной безопасности возможно с применением ниже описанных систем [1].

1. Система предотвращения утечки конфиденциальной информации представляет собой решение, обеспечивающее обнаружение и предотвращения утечки конфиденциальной информации из учреждения по электронным каналам [6, с. 305].

Система обеспечивает защиту от утечки по следующим каналам утечек:

– корпоративная электронная почта (SMTP-канал);

– доступ в сеть Интернет (web-канал);

– сетевые файловые хранилища и папки с общим доступом на рабочих станциях;

– операции на конечных точках сети: копирование/вставка в/из конфиденциального документа; копирование конфиденциальной информации на внешние носители (CD/DVD-диски, USB-накопители и т. п.), контроль печати.

2. Сканеры сетевой безопасности проверяют возможные уязвимости независимо от программной и аппаратной платформы узлов: начиная от рабочих станций, серверов под управлением разнообразных операционных систем и сервисов, работающих на них, заканчивая активным управляемым сетевым оборудованием, на предмет корректной безопасной конфигурации [4, с. 218]. Основные возможности:

– позволяют вести контроль изменений на сканируемых узлах;

– обеспечивают полную идентификацию сервисов на случайных портах;

– эвристический метод определения типов и имен сервисов (HTTP, FTP, SMTP, POP3, DNS, SSH и др.);

– проводят проверку слабости парольной защиты;

– способны выполнить расширенную проверку узлов под управлением Windows;

– глубоко анализируют контент веб-сайтов, структуру HTTP-серверов, проводят проверки на нестандартные DoS-атаки (в последнее время ставшие весьма актуальными);

– оперативно поддерживаются производителями на предмет обновления сигнатур уязвимостей.

3. Система резервного копирования предназначена для автоматизации процессов подразделений эксплуатации, обеспечивающих функционирование автоматизированных систем средствами создания, хранения, управления жизненным циклом и восстановления резервной копии данных за время установленное регламентом резервного копирования. Система обеспечивает решение следующих задач:

– централизованное, на уровне учреждения, автоматизированное управление процедурами резервного копирования, хранения и восстановления данных;

– создание и восстановление резервных копий данных (файлов, баз данных, образов файловых систем) на устройствах хранения данных в инфраструктуре учреждения;

– централизованное автоматизированное управление техническими средствами резервного копирования;

– управление расписанием создания резервных копий;

– управление жизненным циклом резервных копий данных (иерархическое хранение, формирование контрольной суммы, проверка целостности и т. д.);

– централизовано-управляемое восстановление данных;

– выполнение требований по обеспечению информационной безопасности системы резервного копирования.

4. Необходимо создать систему обеспечения сетевой безопасности, основной задачей которой является обеспечение непрерывности функционирования информационно вычислительной системы процессов обработки, хранения и передачи информации в условиях возможных нарушений конфиденциальности, целостности и доступности информационных активов и обеспечивающих их сервисов со стороны каналов связи.

Составляющей этой системы должны быть сертифицированные ФСТЭК средства межсетевого экранирования с технологией организации VPN канала (сертифицированного по ГОСТ 28147–89) для организации INTRANET сети с филиалами и система обнаружения вторжений. В системе обнаружения вторжений заложены способы выявления и предотвращения нарушений политик доступа по своим свойствам и критериям не обрабатываемые межсетевыми экранами [3, с. 173]. Механизмы работы системы многообразны:

– анализ вторжений происходит как по собственной базе угроз, так и без нее, благодаря эвристическим технологиям распознавания протоколов;

– анализ не нормальных отклонений в протоколах;

– оценка функционирования конкретных узлов;

– обнаружение статистических аномалий в потоке данных;

– анализ взаимосвязи происходящих событий.

Эффективная эксплуатация средств возможна только с наличием «подписки» на периодические обновления этих решений, дающие возможность эффективно отражать новые угрозы со стороны всемирной сети.

5. Система терминального доступа предназначена для обеспечения эффективной работы сотрудников учреждения с информационно-аналитическими системами и офисными приложениями в терминальном режиме. Система позволяет добиться:

– снижение совокупной стоимости владения оборудования учреждения;

– повышение надежности и увеличение сроков службы аппаратного обеспечения клиентских рабочих мест;

– повышение производительности труда пользователей и администраторов учреждения;

– повышение уровня информационной безопасности.

При использовании технологии терминального доступа пользователь может быть лишен возможности прямого доступа к файловым серверам и серверам информационно-аналитических систем, минуя терминальный сервер. Таким образом, физическое рабочее место (персональный компьютер) пользователя используется только для взаимодействия между терминальным сервером и ПК в рамках рабочей среды пользователя.

6. Система виртуализации серверов предназначена для повышения коэффициента использования аппаратных ресурсов серверного оборудования, снижения затрат на охлаждение и энергопотребление этого оборудования.

Система обеспечивает следующие преимущества:

– консолидация и унификация аппаратного обеспечения инфраструктурных и прикладных сервисов;

– централизованное управление и разграничение доступа пользователей ПВС;

– повышение уровня отказоустойчивости сервисов, размещенных на ПВС;

– динамическое распределение доступных аппаратных ресурсов между сервисами, размещенными на ПВС, с возможностью их ограничения и резервирования.

7. Система мониторинга телекоммуникационной инфраструктуры предназначена для обеспечения контроля над работой сетевых ресурсов, анализа сетевого трафика между серверами, рабочими станциями, активным сетевым оборудованием [5, с. 562].

Целью внедрения системы является обеспечение доступности ресурсов учреждения, наиболее эффективного использования ресурсов посредством оптимизации их распределения и загрузки, а также повышения производительности работы персонала ИТ-отдела.

8. Единая система управления доступом пользователей к информационным системам предназначена для централизованного управления доступом пользователей к разнообразным автоматизированным информационным системам учреждения. Цели создания системы:

– унификация механизмов и средств управления и контроля над учётными записями пользователей учреждения;

– сокращение объема рутинных операций системных администраторов информационных ресурсов за счёт автоматизации функций по созданию, изменению, удалению учетных записей пользователей;

– контроль отсутствия в учреждении учетных записей уволенных сотрудников; контроль использования учётной записи пользователя при временном отсутствии сотрудника (болезнь, отпуск, командировка);

– централизация процесса аудита учетных записей и присущих им полномочий.

9. Необходимость внедрения единой системы мониторинга информационной безопасности предназначенной для автоматизации контроля информационной безопасности (ИБ) на объекте автоматизации администраторами учреждения. Основными целями внедрения являются:

– повышение эффективности управленческой деятельности и внутреннего контроля организации;

– сокращение временных затрат персонала при выполнении мониторинга ИБ на объекте автоматизации;

– контроль действий пользователей на объекте автоматизации;

– регистрация первичных событий мониторинга, формирование сообщений о событиях ИБ, фиксация коррелированных событий ИБ на основе правил анализа событий ИБ от разнотипных источников данных мониторинга объекта автоматизации, обеспечение возможности создания и редактирования, а также проверки описаний коррелированных событий ИБ на основе информации о событиях ИБ или последовательностей событий ИБ;

– обеспечение централизованного хранения зафиксированной информации о событиях ИБ и коррелированных событиях ИБ, автоматизация извещения персонала о зафиксированных событиях ИБ и коррелированных событиях ИБ.

Предложив меры по обеспечению информационной безопасности учреждения, целесообразно сгруппировать их в три основные категории систем:

1. Система оптимизации ресурсов, в которую входят:

– система виртуализации серверов;

– система терминального доступа.

2. Системы единого управления и мониторинга информационных ресурсов состоящие из:

– единая система управления доступом пользователей к информационным системам;

– единая система мониторинга информационной безопасности;

– система мониторинга телекоммуникационной инфраструктуры.

3. Системы обеспечения информационной безопасности, в которой состоят:

– система резервного копирования;

– система предотвращения утечки конфиденциальной информации;

– сканер сетевой безопасности;

– система обеспечения сетевой безопасности.

Первая категория систем в первую очередь направлена на оптимизацию использования аппаратных средств инфраструктуры учреждения, но при этом вносит вклад в аспекты информационной безопасности.

Вторая категория систем направлена на создание, так называемого, единого интерфейса событий информационной системы учреждения, что, безусловно, дает возможность не упустить из вида критические ситуации, вести централизованный журнал событий, оперативно реагировать на возникающие угрозы информационной безопасности.

В третью категорию систем включены обязательные для внедрения системы и решения. Они помимо своего предназначения позволяют решить вопросы с законодательными требованиями по выполнению мер защиты конфиденциальной информации и персональных данных циркулирующих в информационной сети учреждения [2].

Литература

1. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] // Режим доступа: www.consultant.ru.

2. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах» [Электронный ресурс] // Режим доступа: www.consultant.ru.

3. Зайцев А.П, Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности. Учебное пособие. Изд. 2-е испр. и доп. М.: Машиностроение-1, 2014.

4. Платонов В.В. Программно-аппаратные средства защиты информации. М.: Академия, 2013.

5. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. М.: Гелиос АРВ, 2012

6. Хорев А.А. Способы и средства зашиты информации: Учебное пособие. М.: МО РФ, 2013.