DOI: 10.17117/na.2016.04.03.129

<http://ucom.ru/doc/na.2016.04.03.129.pdf>

Поступила (Received): 04.04.2016

Марченко В.С. Типовая организация защиты информации на предприятии

Marchenko V.S. Modern video surveillance in combination with cloud technology

Предприятие независимо от вида деятельности и формы собственности не в состоянии успешно развиваться и вести хозяйственную деятельность без создания условий функционирования системы защиты информации. В данной статье проанализирован стандартный процесс обеспечения информационной безопасности на предприятии, ценнейшим активом которого является хранимая, обрабатываемая и передаваемая информация
Ключевые слова: информационная безопасность предприятия, информационные угрозы

The company, regardless of activity and form of ownership, is not able to develop successfully and conduct business without creating a system of information protection. This article analyzes the typical process of information security in an enterprise, the most valuable asset of which is stored, processed and transmitted information

Key words: information security of an enterprise, information threats

Марченко Виктория Станиславовна
Кандидат педагогических наук, доцент
Поволжский государственный университет
сервиса
г. Тольятти, ул. Гагарина, 4

Marchenko Viktoria Stanislavovna
Candidate of Pedagogic Sciences, Associate Professor
Volga Region state university of service
Togliatti, Gagarin st., 4

Все предприятия, использующие современные информационные технологии, уделяют значительное внимание обеспечению безопасности своих информационных ресурсов. Убытки, связанные с нарушением работы информационных систем и утратой ценной информации, расходы на восстановление информации и работоспособности информационных систем, компенсации при потере конфиденциальности информации составляют крупные суммы или способны парализовать деятельность любого предприятия.

При осуществлении защиты информации любое предприятие в первую очередь руководствуется правовой составляющей информационной безопасности: Политикой безопасности и рядом процедур, основанных на данном документе. Они регламентируют контроль физического доступа, осуществление логической безопасности, предоставление доступа в Интернет и к электронной почте, осуществление антивирусной защиты программного обеспечения и информации, движущейся на предприятии. Описываются методы резервного копирования данных и способы их шифрования.

Контроль физического доступа необходим, чтобы предотвратить несанкционированный доступ в помещения. Администратор системы должен ежемесячно распечатывать отчет о доступе в кабинеты, где происходит работа с закрытой информацией и отдавать его менеджеру отдела информационных технологий, который просматривает отчет, утверждает и подшивает в соответствующую папку как свидетельство регулярного просмотра доступа. О неавторизованном доступе будет сообщено в службу безопасности для выяснения, почему он был предоставлен. Представители сторонних организаций или поставщики допускаются в помещения отдела информационных технологий только в сопровождении его сотрудника.

Осуществление логической безопасности происходит на основании процедур: пользование паролями, проверка доступа к информационным ресурсам, проверка журналов безопасности и листов безопасности. Очевидно, что схема защиты рассчитана на противодействие попыткам злоумышленников вывести из строя информационную систему или получения доступа к конфиденциальной информации.

Все компьютеры, подключенные к локальной сети и операционные приложения, должны быть защищены. Для ограничения доступа к операционной системе используется регистрационное имя пользователя и пароль. Эта защита должна присутствовать при начальной загрузке компьютера, входе в локальную сеть, в программы и приложения, даже заставка операционной системы тоже должна быть защищена паролем. Регистрационное имя сообщается системным администратором при регистрации нового пользователя. Пользователь должен менять пароли каждые 30 дней. Системный администратор имеет право проверять соответствие паролей и пользователи, чьи пароли не соответствуют требованиям, отключаются от системы. Доступ в сеть разрешается по служебной записке работника с визой руководителя и производится после изменения пароля.

Доступ к информационным ресурсам должен быть разрешенным, контролируемым, регистрируемым и периодически просматриваемым в соответствии с утвержденной процедурой. Они должны использоваться только для выполнения служебных обязанностей. Проверка доступов к обычно происходит по графику. График на год утверждается координатором по информационной безопасности, менеджером отдела информационных технологий и директором. Координатор по информационной безопасности осуществляет проверку подготовленных отчетов на предмет соблюдения принципа разграничения полномочий и оптимального использования лицензий. Он подготавливает Отчеты о доступе пользователей. Сотрудник отдела информационных технологий рассылает руководителям отделов эти Отчеты по графику. После этого отчеты предоставляются руководителям, обязанностью которых является рассмотрение необходимости соответствующих полномочий сотрудникам для выполнения должностных обязанностей.

Системные администраторы ежедневно готовят в электронном виде журналы событий, хранят их в базе данных на сервере, права на которые имеют

только ИТ-специалисты и координаторы. Сформированный журнал подписывается электронным способом, при необходимости добавляется комментарий и отправляется по электронной почте менеджеру отдела информационных технологий на подпись. После этого ему присваивается статус «закрытый». При накоплении значительного объема проводится архивирование журналов в архивной базе данных на сервере.

При проверке листов безопасности администратор осуществляет проверку соответствия параметров требованиям проверочных листов, после чего подшивает и хранит подписанные проверочные листы. Менеджер по информационным технологиям и начальник отдела внутреннего контроля изучают и утверждают исполненные администраторами проверочные листы.

Сотрудники обычно заполняют специальные формы для доступа к различным информационным ресурсам. Пользование Интернетом должно контролироваться, регистрироваться и периодически просматриваться в соответствии с утверждённой процедурой. Доступ к электронной почте должен предоставляться по утверждённому запросу. Пользование электронной почтой контролируется, регистрируется и просматривается в соответствии с определенной процедурой, т. к. использование электронной почты в целях, не связанных с исполнением служебных обязанностей, не допускается.

Антивирусное сканирование производится каждый день на всех компьютерах и серверах. Антивирусный монитор работает постоянно на всех компьютерах и серверах. Антивирусные базы обновляются регулярно согласно утверждённой процедуре или расписанию. Существовать единая точка приёма сообщений об обнаруженных вирусах.

Для борьбы с угрозой потери информации выполняется резервное копирование. Перечень данных, подлежащих резервному копированию, условия и периодичность их копирования составляется и изменяется администраторами системы. Хранение носителей с резервными копиями проходит в соответствии с процедурами. Уничтожение носителей резервного копирования, пришедших в негодность или срок эксплуатации которых истек, является обязательным. Для этого формируется специальная комиссия, которая подписывает Акт, подтверждающий, что носители, приготовленные для уничтожения, действительно не пригодны для дальнейшего использования. Затем эти носители в присутствии членов комиссии уничтожаются так, чтобы никакие данные считать с них было невозможно.

Криптографическое преобразование информации и использование электронно-цифровой подписи присутствует во многих информационных системах. Шифрование обязательно для всей информации, которая хранится или передаётся внутри вычислительных и коммуникационных ресурсов или через внешние сети. Пароли хранятся в зашифрованной форме и передаются тоже с использованием шифрования. Шифрование особенно важно для информации, передаваемой через внешние сети.

Современно оснащенное предприятие хорошо защищает информацию, с которой работает. На всех предприятиях традиционно применяются средства защиты от несанкционированного доступа как в систему, так и в помещения,

ежедневно проводится мониторинг сетей и антивирусного сканирования, работают межсетевые экраны, системы резервного копирования и бесперебойного питания, применяется шифрование данных.

Список используемых источников:

1. Альшанская Т.В., Гурьянова Е.А., Королькова Ю.В. Проблемы информационной безопасности на предприятиях // Развитие науки и образования в современном мире. 2014. С. 97-99.
2. Марченко В.С. Защита экономической информации в коммерческом банке // Информационные системы и технологии: управление и безопасность. Изд-во: ПВГУС, 2014. С. 166-174.

© 2016, Марченко В.С.

Типовая организация защиты информации на предприятии

© 2016, Marchenko V.S.

Modern video surveillance in combination with cloud technology