РАЗДЕЛ XXXIII. ПЕДАГОГИКА

Азиева Л.Д.¹, Садулаева Б.С.²**Преимущества эффективного внедрения систем информационной безопасности в коммерческой компании**¹ФГБОУ ВО «Чеченский государственный университет»²ФГБОУ ВО «Чеченский государственный педагогический университет»

(Россия, Грозный)

doi: 10.18411/lj-07-2020-192

idsp: ljjournal-07-2020-192

Аннотация

В наше время достаточно трудно найти организации или предприятия (даже самые малые), которые не обладали бы современными средствами обработки и передачи данных. Обеспечение информационной безопасности помогает защитить информацию и информационную инфраструктуру предприятия от негативных воздействий.

Важно пояснять сотрудникам, что выполнение правил по информационной безопасности это норма поведения, расширять их кругозор в области безопасности использования конфиденциальной информации, рассказывать на ежемесячной основе о существующих новых методах защиты, обучать сотрудников дистанционно на основе электронных обучающих курсов и содержать методы обязательного контроля. [4]

Ключевые слова: информационная безопасность организации, образовательные программы повышения квалификации, цифровой контент организации.

Abstract

Nowadays it is quite difficult to find organizations or enterprises (even the smallest ones) that would not have modern means of processing and transmitting data. Providing information security helps protect the information and information infrastructure of the enterprise from negative influences.

It is important to explain to employees that the implementation of information security rules is the norm of behavior, broaden their horizons in the field of security of using confidential information, talk on a monthly basis about existing new protection methods, train employees remotely based on electronic training courses and contain mandatory monitoring methods. [4]

Keywords: information security of the organization; educational programs for continuing education; digital content of the organization.

Возможные пути проникновения вредоносных программ в компьютерную сеть компании:

- сеть Интернет, путем загрузки пользователями зараженного программного обеспечения;
- загрузка WWW-страниц с активными приложениями,
- содержащими вредоносный код;
- заражение рабочих станций пользователей через электронную почту;
- распространение вредоносных программ через сеть Интернет и электронную почту посредством использования уязвимостей программного обеспечения;
- установка на рабочие станции и сервера предприятия зараженного программного обеспечения или электронных документов.

Что может произойти, когда вредоносная программа распространяется в корпоративной компьютерной сети:

- изменение, уничтожение данных;
- утрата информации из компьютерной сети предприятия;
- нарушение технологических процессов в компьютерной сети предприятия.

Выполнение всеми сотрудниками предприятия мероприятий, направленных на предотвращение проникновения вредоносных программ в компьютерную сеть предприятия, является основой нормального функционирования сети и одним из важнейших условий информационной безопасности. [3]

Должен соблюдаться антивирусный контроль, который автоматически обновляет антивирусные базы на всех компьютерах ваших сотрудников. Использование общих дисковых ресурсов на компьютере должно быть разрешено только при наличии разрешения в соответствии с предварительно определенным свободным пространством. Использование на компьютерах накопителей со съемными компьютерными носителями и портами USB должны быть разрешены в случаях в соответствии с заранее установленными допусками.

Компьютеры, хранящие конфиденциальные данные на жестких дисках, должны быть защищены программными и аппаратными системами. Сохраненная база данных может быть криптографически защищена для защиты информации от несанкционированного доступа.

Сотрудникам финансового предприятия необходимо запретить:

- входить в компьютерную сеть предприятия, используя чужой логин и пароль;
- оставлять без присмотра не заблокированный монитор компьютера;
- самостоятельно изменять аппаратную или программную конфигурацию компьютера;
- самостоятельно устанавливать на компьютер программное обеспечение;
- разрешать другим лицам работу на компьютере со своими правами доступа;
- запрещается загружать из сети Интернет программное обеспечение;
- запрещается отключать антивирусное программное обеспечение, установленное на компьютере, и изменять его настройки.

Пользователь компьютерной сети предприятия должен:

- соблюдать требования регламентирующих документов по информационной безопасности;
- использовать персональный компьютер и ресурсы компьютерной сети предприятия только для выполнения своих прямых служебных обязанностей;
- сохранять рабочие материалы и документы в электронном виде в специально выделенном каталоге файлового сервера;
- блокировать монитор компьютера при потребности покинуть рабочее место, даже при кратковременном отсутствии;
- выключать рабочую станцию при уходе с рабочего места. [1]

Прежде чем перейти к списку обязательных требований, которые должны быть представлены в паролях, используемых сотрудниками компании в сети компании, обратимся к документации, описывающей эти требования - политика паролей компании. Это должно быть частью комплексной политики безопасности предприятия. Комплексная политика должна включать в себя основные требования и положения, на основании которых составляется должностная инструкция работника, указывается предмет в трудовом договоре и т. д.

Информация о пароле пользователя является конфиденциальной информацией, которая используется для идентификации и доступа к информационным ресурсам каждого отдельного пользователя. [3]

Операционные системы серверов должны быть настроены таким образом, чтобы исключить возможность ознакомления с парольной информацией любого из пользователей, включая Администратора. Серверы должны быть защищены паролем на загрузку операционной системы и доступа к конфигурации BIOS. Компьютеры рабочих станций должны быть защищены паролем на доступ к конфигурации BIOS. Компьютеры рабочих станций, на которых хранятся конфиденциальные сведения, должны быть защищены паролем на загрузку операционной системы.

Когда сотрудник организации уходит в отпуск, системный администратор блокирует имя пользователя в информационной системе компании на основе приложения во главе организационной единицы.

Когда сотрудник увольняется из организации, системный администратор удаляет имя пользователя в корпоративной информационной системе на основе страницы обхода.

Период действия паролей составляет 90 суток, после чего они подлежат замене на новые, ранее не применявшиеся.

Администраторы различных информационных систем не управляют паролем администратора при повседневной деятельности, которые не управляются с помощью административных функций. Для этого администраторам необходимо дать пароль с правами пользователя.

Пароли Администраторов и пароли BIOS серверов должны храниться в опечатанных конвертах в сейфе директора предприятия. Каждый пароль хранится в отдельном конверте.

Доступ в компьютерную сеть предприятия, через общедоступные каналы связи обеспечивается только с применением смарт-карт либо их полнофункциональных аналогов USB-брелков eToken.

Неверная информация, связанная с нарушениями доступа к компьютерной сети, рассматриваются как нарушения режима информационной безопасности и анализируются через процедуру служебного расследования.

Ответственным за настройку серверов и рабочих станций является администратор компьютерной сети.

Под компьютерными вирусами, троянами, следует понимать программы, которые могут сохранять способность воспроизводить больше (вредоносные программы) и добавлять свои собственные измененные, возможно, измененные копии в другие программы. [3]

Правила антивирусной защиты доводятся до всех пользователей компьютерной сети предприятия под личную роспись в журнале инструктажа администратором сети.

При передаче программного обеспечения и электронных документов в другие предприятия или физическим лицам необходимо проводить антивирусный контроль передаваемой информации.

Все факты проникновения вредоносных программ в компьютерную сеть предприятия являются нарушением информационной безопасности и подлежат служебному расследованию.

Контроль выполнения антивирусной безопасности пользователями компьютерной сети предприятия возлагается на информационно-технический отдел. [3]

Электронный контент — сведения, а также продукты и относящиеся к ним услуги, предоставляемые абонентам сетей передачи данных и сетей сотовой связи в электронном (цифровом) виде, потребляемые и используемые с применением устройств обработки цифровой информации.

Под «электронным информационным материалом» могут подразумеваться практически любые сведения, размещённые на электронном (цифровом) носителе информации: текст или же аудио-, видео-, фото файлы. [4]

Рассмотрим ниже инструменты для создания электронных учебных материалов.

CourseLab – это внушительное и вместе с тем легкодоступное в эксплуатации средство для формирования интерактивных цифровых курсов, создаваемых для использования в сети Интернет или на съёмных носителях, в системах удаленного или внутрикорпоративного обучения.

Благодаря CourseLab можно создавать и редактировать электронный курс в среде WYSIWYG, не обладая знаниями в области языков программирования.

Бесплатную англоязычную версию CourseLab можно скачать на официальном сайте. На русскоязычном ресурсе – ознакомиться с прилагаемым проектным материалом или купить русскую версию продукта.

Сайт - это цифровой контент, который представляет любую компанию или отдельное лицо в Интернете. Сайт также представляет собой современную и продвинутую способность передавать информацию, являясь средством коммуникации и, наконец, рекламным продуктом, который предлагает большие возможности в области поиска и привлечения потребителей, заинтересованных в ресурсах.

Компетентная и качественная разработка, изготовление специализированного сайта решает сразу множество задач:

- обучение сотрудников правилам информационной безопасности;
- создание и укрепление стиля и имиджа;
- увеличение и расширение обучаемой аудитории;
- увеличение доходов фирмы или компании (за счет сокращения командировок);
- увеличение количества и качества передачи информации между компаниями и сотрудниками.

Создание Web-сайтов является одной из важнейших технологий разработки ресурсов Интернет. Web-страница представляет собой текстовый файл с расширением *.htm, который содержит текстовую информацию и специальные команды - HTML-коды, определяющие, в каком виде данные будут отображаться в окне браузера. Вся графическая, аудио- и видео информация непосредственно в Web-страницу не входит и представляет собой отдельные файлы с расширениями (*.gif, *.jpg, *.mp3, *.avi и т.д.). Качественный сайт, содержащий в себе все полезные данные, является лучшей визитной карточкой и коммерческой фирмы, и образовательных структур, работая на них круглосуточно.

Web-сайты дают возможность:

- анализировать спрос, мысли и выбор потребителей, кейс их знаний об определенных товарах, услугах и фирмах;
- формировать совместные проекты и курсы с отдаленной командой исполнителей;
- выполнять внутрифирменное повышение квалификации персонала или внутрикорпоративное обучение сотрудников предприятия;
- формировать коллективные приоритеты и нормы поведения, разъяснять политику, проводимую предприятием, облегчать взаимосвязь руководителей и сотрудников.

Цифровая среда имеет ряд очевидных плюсов и возможностей, среди которых:

- интерактивный характер коммуникации;
- постоянная доступность информации;

- постоянное обновление информации, дополнение с учетом запросов или предложений клиентов сайта;
- предоставление высоких объемов данных, а именно текстовой и графической, звуковой и видеоинформации. [2]

Ленточная панель управления напоминает Microsoft Office, что значительно облегчает освоение сервиса и создание ментальной карты. Ментальная карта памяти – это диаграмма, которая знакомит пользователя сервиса с концепцией, назначением или другими объектами, связанными и расположенными вокруг ключевых слов, идеи или плана. Эти карты используются для формирования, представления информации, структурирования идеи, как вспомогательные средства в учебе, организациях, решении проблем и принятия решений. [2]

При использовании методов работы с картами памяти, выявляются явные плюсы:

- карты памяти помогают легко запомнить информацию, так как она структурирована;
- карты памяти облегчают визуальное восприятие и понимание вопроса, существует возможность вставки рисунков и записок;
- карты памяти раскрывают информацию, под каждой темой можно создавать подтемы и после просмотра общей картины перейти к более детальному изучению вопроса.

Сервис Mindomo это идеальный вариант для создания цифрового контента, так как позволяет создать карту памяти на безвозмездной основе, не скачивая и не предустанавливая программное обеспечение, работать с сервисом можно онлайн. Для работы или ознакомления с приложением необходимо перейти на официальный сайт <http://m.mindomo.com/>

Каждая публичная карта, созданная Mindomo, имеет уникальный адрес, который можно использовать на страницах HTML, чтобы указать ссылку на необходимую карту или пригласить других пользователей к совместной работе. Можно связывать карты со своей домашней страницей или отправить их другим пользователям для ознакомления, приглашение направляется по электронной почте.

Цифровой создатель должен иметь профессиональную квалификацию в области информационных и коммуникационных технологий, программного и аппаратного обеспечения, с другой стороны, он должен иметь высококачественное образование в области научных исследований, знать характеристики предметной области и иметь профессиональную квалификацию для обработки семантической информации.

Цифровой контент обеспечивает необходимые предпосылки для предотвращения информационных угроз, оптимизации затрат на информационную безопасность, снижения риска репутации компании и повышения прибыльности компании.

1. Вдовин, В.М. Информационные технологии в финансово-банковской сфере: Практикум / В.М. Вдовин. - М.: Дашков и К, 2012. - 248 с.
2. Олейник, П.П. Корпоративные информационные системы: учебник для вузов. Стандарт третьего поколения / П.П.Олейник. – СПб: Питер, 2012. – 176 с.
3. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
4. Юсупова Л.В., Садулаева Б.С. Реализация дистанционных технологий в условиях информационно-образовательной среды вуза. Известие Чеченского государственного университета. №4(8), 2017, С.44-48.