МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

Кафедра информационных систем

УТВЕРЖДАЮ
Заведующий кафедрой ИС

«___» 20___ г.

ЛЕКЦИЯ №11
по учебной дисциплине
«Системы электронного документооборота»
для студентов направления подготовки 38.03.01 «Экономика»
(для всех профилей подготовки)

Тема №4
Юридически значимый электронный документооборот

Занятие №1
Понятие юридически значимого электронного документооборота

Рассмотрена и одобрена на заседании кафедры ИС
Протокол №_____
« _____ » _____ 20___ г.

Ставрополь, 2022

Цель:

1. Сформировать информационно-наглядное представление о юридически значимой системе электронного документооборота.
2. Изучить процедуры авторизации, идентификации и аутентификации реализуемые в ходе электронного документооборота.
3. Уяснить особенности процедур обработки информации в локальных вычислительных сетях.

Время: _____90 мин.

Учебно-материальное обеспечение:

1. ГОС ВО по направлению.
2. Рабочая программа дисциплины.
3. Тематика семестровых домашних заданий.
4. Основная и дополнительная литература.

Распределение времени

I.	Вступительная часть	5 мин.
II.	Основная часть	
	Учебные вопросы:	
1.	Общая характеристика электронного документооборота	40 мин.
2.	Идентификация и аутентификация пользователей в системе электронного документооборота	40 мин.
3.	Общие требования и рекомендации по защите информации в ЛВС	40 мин.
III	Заключительная часть	5 мин.

Вводная часть

В рамках деятельности коммерческих организаций и государственных учреждений документы являются универсальным носителем информации. Они используются в качестве инструмента управления и выполняют функцию обеспечения взаимодействия между внутренними и/или внешними контрагентами: отдельными сотрудниками, целыми подразделениями, клиентами, партнерами и вышестоящими инстанциями. Все задействованные в бизнес процессах сотрудники, как рядовые специалисты, так и топ-менеджеры, принимают участие в создании, обработке, хранении и распространении документов. Эффективность постановки и внедрения документооборота влияет на качество работы всего предприятия в целом.

Первый учебный вопрос - Общая характеристика электронного документооборота.

По оценке известного европейского эксперта Бруно Коха, в 2011г. примерно 5 млн. европейских предприятий уже вовлечены в электронный документооборот со счетами и счетами-фактурами. В 2008г. таких предприятий было 1,7 млн., то есть за три года их количество выросло в три раза.

Количество счетов-фактур, выставляемых в России и Европе, примерно одинаково. По разным оценкам это от 15 до 17 млрд документов в год. По словам Коха, на сегодняшний день 50 % российских компаний уже имеет ЭЦП, при этом в России, в отличие от Европы, единое законодательство и преимущественно один язык. Все эти факторы позволяют развиваться российскому рынку электронных счетов-фактур в 5 раз быстрее, чем европейскому.

Цели внедрения электронного документооборота

Существует более 20 вариантов определения понятия «документооборот». Наиболее точной и полной является формулировка, представляющая собой цикличное правило:

«записывать -> делать -> контролировать -> анализировать -> записывать».

Электронный документооборот (СЭД) позволяет обеспечить поддержку делопроизводства посредством внедрения компьютерных технологий. Регламентация и контроль процесса движения внешних и внутренних документов на предприятии основываются на работе информационных систем.

Основное назначение документооборота заключается в постановке работы с информацией, которая обрабатывается внутри и вне предприятия. Этот процесс включает в себя поиск, сбор, консолидацию, публикацию и использование знаний. ***Таким образом, высшей ценностью СЭД является систематизация информационных потоков.*** В качестве преимущества внедрения систем электронного документооборота на предприятии выделяют окупаемость знаний и/или информации – return on knowledge (ROK) и/или return on information (ROI).

В перечень причин для перехода к СЭД входят следующие организационные цели.

Формирование единого информационного пространства. Создание единого пространства для хранения, обработки и многократного использования информации обеспечивает вовлеченность всех сотрудников организации в процесс коллективной работы. Функционал СЭД позволяет фиксировать и вести последовательный учет данных о том, какой именно сотрудник, сколько раз и какую информацию добавляет в общую базу. Информационное пространство программы исключают необходимость

хранения документов на локальном компьютере. С помощью такой системы руководитель предприятия может отслеживать фактическую деятельность каждого работника.

Стандартизация работы с документами. Единый для всех сотрудников регламент устанавливает четкий порядок процедур, на основе которых обрабатывается электронный вариант документа. Стандартизация процессов позволяет обеспечить доступность, управляемость и защищенность информации. Технологии делопроизводства унифицируются и систематизируются, обретая единую форму исполнения. Благодаря стандартизации процессов обработки документов на предприятии создается возможность оповещения об их создании и изменении, а также производится своевременная автоматическая доставка ответственным лицам.

Документальное сопровождение бизнес процессов. Внедрение СЭД способствует созданию качественно новой системы управления на основе соблюдения электронных регламентов. Администрация компании определяет параметры процессов и применяет формальные методики для их описания. Электронное сопровождение бизнес процессов создает ряд конкурентных преимуществ:

наличие четко определенного регламентированного комплекса действий с фиксацией изменяющихся в процессе их выполнения результатов;

обеспечение немедленного информирования о нарушениях или несоответствиях в рамках деятельности компании;

возможность своевременного внесения актуальных корректировок, способствующих повышению эффективности процессов.

Одновременно с этим решаются вопросы достоверности информации, которая содержится во входящей и исходящей документации, а также скорости ее передачи.

Повышение эффективности управления организацией. Цель достигается за счет обеспечения прозрачности процессов на предприятии. Перевод делопроизводства на «электронный режим» и строгий контроль соблюдения сотрудниками своих должностных обязанностей осуществляется на всех уровнях управления. Электронный документооборот обеспечивает эффективность накопления информационных ресурсов компании и доступа к ним персонала.

Упрощение процессов поиска и хранения документации. СЭД позволяет сократить циклы документооборота в организации, временные затраты на контроль выполнения функций. Облегчается процесс принятия управленческих решений. Электронное делопроизводство помогает повысить эффективность поиска и хранения данных, обеспечивая полноту, качество и надежность используемой информации. Упрощается работа с архивными данными, ускоряется получение сведений об актуальном состоянии процессов организации, в которых участвует тот или иной электронный документ.

Сокращение бумажного документооборота. Снижение доли бумажного документооборота в делопроизводстве компании позволяет экономить материальные и людские ресурсы. Удешевление процесса

управления потоками деловой документации позволяет экономить время и средства для исполнения сотрудниками прямых должностных обязанностей. Хранение электронных версий документов не только снижает расход бумаги, но и значительно упрощает работу с информацией. Например, документы можно распечатывать только по мере необходимости.

Обеспечение сохранности информации. Внедрение СЭД и параллельное выстраивание общей культуры работы со служебной документацией позволяют контролировать доступ к информации. Это обеспечивает возможность выявлять случаи несанкционированного использования данных. В условиях хранения больших объемов информации электронное делопроизводство повышает эффективность работы специалистов, отвечающих за ликвидацию утечки информации.

Отслеживание взаимоотношений с контрагентами. Электронный документооборот создает отлаженный механизм фиксирования, хранения и отслеживания информации о взаимоотношениях компании с разными категориями контрагентов. В общей базе могут содержаться данные не только о сотрудниках организации, но и корреспонденция, связанная с поставщиками и клиентами.

Перечисленные преимущества внедрения СЭД позволяют рассматривать электронный документооборот не только как технологический, но и как организационный инструмент управления компанией

Второй учебный вопрос - Идентификация и аутентификация пользователей в системе электронного документооборота

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Эту информацию называют идентификатором субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию. Идентификация (Identification) - это процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование (Accounting) - это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Хотя эта

учетная информация может быть использована для выписывания счета, с позиций безопасности она особенно важна для обнаружения, анализа инцидентов безопасности в сети и соответствующего реагирования на них. Записи в системном журнале, аудиторские проверки и администрирование ПО - все это может быть использовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные Web-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации. Примером слабой формы аутентификации может служить использование IP-адреса для определения пользователя. Подмена (spoofing) IP-адреса может легко разрушить этот механизм аутентификации. Надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получат доступ к контролируемой информации.

При защите каналов передачи данных должна выполняться взаимная аутентификация субъектов, то есть взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса в процессе установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры - обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Одной из распространенных схем аутентификации является простая аутентификация, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств его использования и обработки. Аутентификация на основе многоразовых паролей является простым и наглядным примером использования разделяемой информации. Пока в большинстве защищенных виртуальных сетей VPN (Virtual Private Network) доступ клиента к серверу разрешается по паролю. Однако все чаще применяются более эффективные средства аутентификации, например программные и аппаратные системы аутентификации на основе одноразовых паролей, смарт-карт, PIN-кодов и цифровых сертификатов.

Пароль — это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Персональный идентификационный номер PIN является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN-кода должно быть известно только держателю карты.

Базовый принцип «единого входа» предполагает достаточность одноразового прохождения пользователем процедуры аутентификации для доступа ко всем сетевым ресурсам. Поэтому в современных операционных системах предусматривается централизованная служба аутентификации,

которая выполняется одним из серверов сети и использует для своей работы базу данных. В этой базе данных хранятся учетные данные о пользователях сети. В эти учетные данные наряду с другой информацией включены идентификаторы и пароли пользователей.

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. При попытке логического входа в сеть пользователь набирает на клавиатуре компьютера свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись, из нее извлекается пароль и сравнивается с тем паролем, который ввел пользователь. Если они совпали, то аутентификация прошла успешно, пользователь получает легальный статус, а также права и ресурсы сети, которые определены для его статуса системой авторизации.

Схема простой аутентификации с использованием пароля показана на рисунке 6.1. Очевидно, что вариант аутентификации с передачей пароля пользователя в незашифрованном виде не гарантирует даже минимального уровня безопасности, так как подвержен многочисленным атакам и легко компрометируется. Чтобы защитить пароль, его нужно зашифровать перед пересылкой по незащищенному каналу. Для этого в схему включены средства шифрования $E_к$ и расшифрования D_K, управляемые разделяемым секретным ключом К. Проверка подлинности пользователя основана на сравнении присланного пользователем пароля P_A и исходного значения P_A, хранящегося на сервере аутентификации. Если значения P_A и P_A' совпадают, то пароль P_A считается подлинным, а пользователь А - законным.

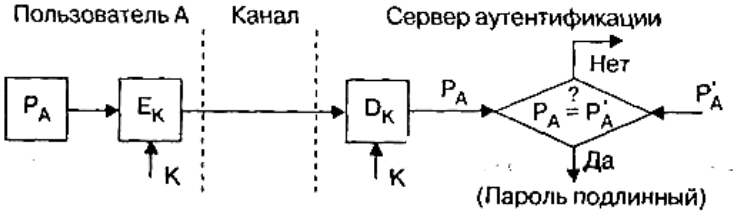

Рисунок 1 - Простая аутентификация с использованием пароля

где Р - пароль пользователя;

ID - идентификатор пользователя;

E_P — процедура шифрования, выполняемая с использованием пароля Р в качестве ключа

Схемы организации простой аутентификации отличаются не только методами передачи паролей, но и видами их хранения и проверки. Наиболее распространенным способом является хранение паролей пользователей в открытом виде в системных файлах, причем на эти файлы устанавливаются атрибуты защиты от чтения и записи (например, при помощи описания соответствующих привилегий в списках контроля доступа операционной системы). Система сопоставляет введенный пользователем пароль с хранящейся в файле паролей записью. При этом способе не используются криптографические механизмы, такие как шифрование или однонаправленные

функции. Очевидным недостатком данного способа является возможность получения злоумышленником в системе привилегий администратора, включая права доступа к системным файлам и, в частности, к файлу паролей.

Для обеспечения надежной защиты операционной системы пароль каждого пользователя должен быть известен только этому пользователю и никому другому, в том числе и администраторам системы. На первый взгляд то, что администратор знает пароль некоторого пользователя, не отражается негативно на безопасности системы, поскольку администратор, войдя в систему от имени обычного пользователя, получает права, меньшие, чем те, которые он получит, зайдя в систему от своего имени. Однако, входя в систему от имени другого пользователя, администратор получает возможность обходить систему аудита, а также совершать действия, компрометирующие этого пользователя, что недопустимо в защищенной системе. Таким образом, пароли пользователей не должны храниться в операционной системе в открытом виде.

Схемы аутентификации, основанные на традиционных многоразовых паролях, не обладают достаточной безопасностью. Такие пароли можно перехватить, разгадать, подсмотреть или просто украсть. Более надежными являются процедуры аутентификации на основе одноразовых паролей.

Суть схемы одноразовых паролей — использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, и затем его действие истекает. Даже если кто-то перехватил его, пароль окажется бесполезен. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от угроз извне. Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей.

Известны следующие методы применения одноразовых паролей для аутентификации пользователей:

1. Использование механизма временных меток на основе системы единого времени.
2. Использование списка случайных паролей, общего для легального пользователя и проверяющего, и надежного механизма их синхронизации.
3. Использование генератора псевдослучайных чисел, общего для пользователя и проверяющего, с одним и тем же начальным значением.

Генерация одноразовых паролей может осуществляться аппаратным или программным способом. Некоторые аппаратные средства доступа на основе одноразовых паролей реализуются в виде миниатюрных устройств со встроенным микропроцессором, внешне похожих на платежные пластиковые карточки. Такие карты, обычно называемые ключами, могут иметь клавиатуру и небольшой дисплей.

В качестве примера реализации первого метода рассмотрим технологию аутентификации SecurlD на основе одноразовых паролей с использованием аппаратных ключей и механизма временной синхронизации. Эта технология аутентификации разработана компанией Security Dynamics и реализована в

коммуникационных серверах ряда компаний, в частности в серверах компании Cisco Systems и др. Схема аутентификации с использованием временной синхронизации базируется на алгоритме генерации случайных чисел через определенный интервал времени. Этот интервал устанавливается и может быть изменен администратором сети. Схема аутентификации использует два параметра:

- секретный ключ, представляющий собой уникальное 64-битовое число, назначаемое каждому пользователю и хранящееся в базе данных аутентификационного сервера и в аппаратном ключе пользователя;
- значение текущего времени.

Когда удаленный пользователь делает попытку логического входа в сеть, ему предлагается ввести его персональный идентификационный номер PIN, состоящий из четырех десятичных цифр, а также шесть цифр случайного числа, отображаемого в этот момент на дисплее аппаратного ключа. Используя введенный пользователем PIN-код, сервер извлекает из базы данных секретный ключ пользователя и выполняет алгоритм генерации случайного числа, используя в качестве параметров извлеченный секретный ключ и значение текущего времени. Затем сервер проверяет, совпадают ли сгенерированное число и число, введенное пользователем. Если эти числа совпадают, то сервер разрешает пользователю осуществить логический вход в систему.

Второй метод применения одноразовых паролей для аутентификации пользователей основан на использовании списка случайных паролей, общего для пользователя и проверяющего, и надежного механизма их синхронизации. Разделяемый список одноразовых паролей представляется в виде последовательности или набора секретных паролей, где каждый пароль употребляется только один раз. Данный список должен быть заранее распределен между сторонами аутентификационного обмена. Вариантом данного метода является использование таблицы запросов-ответов, в которой содержатся запросы и ответы, используемые сторонами для проведения аутентификации, причем каждая пара должна применяться только один раз.

Третий метод применения одноразовых паролей для аутентификации пользователей основан на использовании генератора псевдослучайных чисел, общего для пользователя и проверяющего, с одним и тем же начальным значением. Известны следующие варианты реализации этого метода:

- последовательность преобразуемых одноразовых паролей. В ходе очередной сессии аутентификации пользователь создает и передает пароль именно для данной сессии, зашифрованный на секретном ключе, полученном из пароля предыдущей сессии;
- последовательности паролей, основанные на односторонней функции. Суть данного метода составляет последовательное использование односторонней функции (известная схема Лампорта). Этот метод является более предпочтительным с точки зрения безопасности по сравнению с методом последовательно преобразуемых паролей.

Одним из наиболее распространенных протоколов аутентификации на основе одноразовых паролей является стандартизованный в Интернете протокол S/Key (RFC 1760). Данный протокол реализован во многих системах, требующих проверки подлинности удаленных пользователей, в частности в системе TACACS+ компании Cisco.

Третий учебный вопрос - Общие требования и рекомендации по защите информации в ЛВС

Характерными особенностями локальной вычислительной сети (ЛВС) являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного сопровождения со стороны администратора безопасности информации.

Информация, составляющая служебную тайну, и персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны.

Класс защищенности ЛВС определяется в соответствии с требованиями РД ГТК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам могут быть назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации.

Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи.

Положения данного раздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Интернет.

Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

- в АС класса 1Г - МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

ЗАЩИТА ИНФОРМАЦИИ ПРИ РАБОТЕ С СИСТЕМАМИ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

– в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;

– БД могут быть физически распределены по различным устройствам и узлам сети;

– БД могут включать информацию различного уровня конфиденциальности;

– разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;

– разграничение доступа пользователей к объектам БД - таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п. - может осуществляться только средствами СУБД;

– регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД;

– СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

С учетом указанных особенностей при создании БД рекомендуется:

– при выборе СУБД ориентироваться на операционные системы и СУБД, либо включающие штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;

– при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;

– при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

Защита информации при взаимодействии абонентов с сетями общего пользования

В настоящем разделе приведены рекомендации, определяющие условия и порядок подключения абонентов к информационным сетям общего пользования (глобальным), а также рекомендации по обеспечению безопасности конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой

определяет собственник этих ресурсов (коммерческая тайна), при подключении и взаимодействии абонентов с этими сетями.

Данные рекомендации определены, исходя из требований РД ГТК «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», а также из учета следующих основных угроз безопасности информации, возникающих при взаимодействии с глобальной сетью:

– несанкционированный доступ к информации, хранящейся и обрабатываемой во внутренних ЛВС (на серверах, рабочих станциях) или на персональных компьютерах, как из глобальной сети, так и из внутренних ЛВС;

– доступ к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу, Web/proxy-серверу), соединяющему внутренние ЛВС компании с глобальной сетью;

– несанкционированный доступ к данным (сообщениям), передаваемым между внутренними ЛВС и глобальной сетью, включая их модификацию, имитацию и уничтожение;

– заражение программного обеспечения компьютерными вирусами из глобальной сети как путем приема зараженных файлов, так и посредством электронной почты, Java-апплетов и объектов ActiveX;

– внедрение программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с глобальной сетью;

– несанкционированная передача защищаемой конфиденциальной информации ЛВС в глобальную сеть;

– возможность перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

Условия подключения абонентов к глобальной сети

Подключение к глобальной сети абонентского пункта (АП) осуществляется по решению руководителя компании на основании соответствующего обоснования. Обоснование необходимости подключения АП к глобальной сети должно содержать:

– наименование сети, к которой осуществляется подключение, и реквизиты организации-владельца и провайдера сети;

– состав технических средств для оборудования АП;

– предполагаемые виды работ и используемые прикладные сервисы глобальной сети (электронная почта, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента в частности;

– режим подключения АП и абонентов к глобальной сети (постоянный, в том числе круглосуточный, временный);

– состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - браузеры и т.п.);

– число и перечень предполагаемых абонентов (диапазон используемых IP-

адресов);

– меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, конфигурация, правила работы с ними;

– перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из глобальной сети.

Право подключения к глобальной сети АП, не оборудованного средствами защиты информации от НСД, может быть предоставлено только в случае обработки на АП информации с открытым доступом, оформленной в установленном порядке как разрешенной к открытому опубликованию. В этом случае к АП, представляющим собой персональные компьютеры с модемом, специальные требования по защите информации от НСД не предъявляются.

Подключение к глобальной сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД.

Порядок подключения и взаимодействия абонентских пунктов с глобальной сетью, требования и рекомендации по обеспечению безопасности информации

Подключение АП к глобальной сети должно осуществляться в установленном порядке через провайдера сети.

Подключение ЛВС компании к глобальной сети должно осуществляться через средства разграничения доступа в виде МЭ. Не допускается подключение ЛВС к глобальной сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления МЭ должны быть исключены из конфигурации.

АП с помощью МЭ должен обеспечивать создание сеансов связи абонентов с серверами глобальной сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

При использовании почтового и Web-сервера компании последние не должны входить в состав ЛВС АП и должны подключаться к глобальной сети по отдельному сетевому фрагменту (через маршрутизатор).

На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к глобальной сети (обоснование может корректироваться в установленном в компании порядке).

Не допускается активизация не включенных в обоснование прикладных серверов (протоколов) и не требующих привязок протоколов к портам.

Установку программного обеспечения, обеспечивающего функционирование АП, должны выполнять уполномоченные специалисты под контролем администратора. Абоненты АП не имеют права производить

самостоятельную установку и модификацию указанного программного обеспечения, однако могут обращаться к администратору для проведения экспертизы на предмет улучшения характеристик, наличия вирусов, замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения целиком ложится на абонента АП. При обнаружении фактов такого рода администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить рабочее место абонента от глобальной сети и ЛВС и поставить об этом в известность руководство.

Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

СЗИ НСД, устанавливаемая на персональные компьютеры, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

– идентификацию и аутентификацию пользователей при доступе к компьютерам, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;

– контроль доступа к ресурсам компьютеров, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;

– регистрацию доступа к ресурсам компьютеров, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

– регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ НСД должна быть целостной, то есть защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

Технические средства АП должны быть размещены либо в отдельном помещении (если компьютеры подключены к глобальной сети), либо в рабочих помещениях абонентов с принятием организационных и технических мер, исключающих несанкционированную работу в глобальной сети. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки

зрения электроакустики. В нерабочее время помещение с компьютерами либо с соответствующим сервером сдается под охрану в установленном порядке.

При создании АП рекомендуется:

– по возможности размещать МЭ для связи с внешними сетями, Web-серверы, почтовые серверы в отдельном защищенном помещении (ЗП), доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы). Периодически проверять работоспособность МЭ с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не следует устанавливать на МЭ какие-либо другие прикладные сервисы (СУБД, почтовые сервисы и т.п.);

– при предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. Тем пользователям АП, которым не требуются услуги глобальной сети, не предоставлять их. Пользователям, которым необходима лишь электронная почта, предоставлять только доступ к ней. Максимальный перечень предоставляемых прикладных сервисов ограничивать следующими: электронная почта, FTP, HTTP, Telnet;

– использовать операционные системы со встроенными функциями защиты информации от НСД или сертифицированные СЗИ НСД;

– эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов;

– в целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации осуществлять анализ принимаемой из глобальной сети и передаваемой в нее информации, в том числе на наличие вирусов. Копии исходящих сообщений электронной почты и отсылаемых в глобальную сеть файлов следует направлять в адрес защищенного архива АП для последующего анализа со стороны администратора (службы безопасности);

– проводить постоянный контроль информации, помещаемой на Web-серверы предприятия. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

Приказом руководства компании назначаются лица (абоненты), допущенные к работе в глобальной сети с соответствующими полномочиями, а также лица, ответственные за эксплуатацию указанного АП и контроль за выполнением мероприятий по обеспечению безопасности информации при работе абонентов в глобальной сети (руководители подразделений и администраторы).

Вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей:

– порядок подключения и регистрации абонентов в глобальной сети;

– порядок установки и конфигурирования на АП общесистемного,

прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов), их новых версий;

– порядок применения средств защиты информации от НСД на АП при взаимодействии абонентов с глобальной сетью;

– порядок работы абонентов в глобальной сети, в том числе с электронной почтой, порядок выбора и доступа к внутренним и внешним Web-серверам;

– порядок оформления разрешений на отправку данных в глобальную сеть (при необходимости);

– обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с глобальной сетью;

– порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов глобальной сети.

К работе в качестве абонентов глобальной сети допускается круг пользователей, ознакомленных с требованиями по взаимодействию с другими абонентами глобальной сети и обеспечению при этом безопасности информации. Такие пользователи допускаются к самостоятельной работе в глобальной сети после сдачи соответствующего зачета.

Абоненты глобальной сети обязаны:

– знать порядок регистрации и взаимодействия в глобальной сети;

– знать инструкцию по обеспечению безопасности информации на АП;

– знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);

– уметь пользоваться средствами антивирусной защиты;

– после окончания работы в глобальной сети проверить свое рабочее место на наличие вирусов.

Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в глобальной сети носители информации учитываются в журналах несекретного делопроизводства. При этом на корпусе (конверте) носителя информации наносится предупреждающая маркировка: «Допускается использование только в Сети».

Для приемки в эксплуатацию АП, подключаемого к глобальной сети, приказом руководства компании назначается аттестационная комиссия, проверяющая выполнение установленных требований и рекомендаций. Аттестационная комиссия в своей работе руководствуется требованиями и рекомендациями настоящего документа.

По результатам работы комиссии оформляется заключение, в котором отражаются следующие сведения:

– типы и номера выделенных технических средств АП, в том числе каждого абонента, их состав и конфигурация;

– состав общего и сервисного прикладного коммуникационного программного обеспечения (ОС, маршрутизаторов, серверов, межсетевых экранов, браузеров и т.п.) на АП в целом и на каждой рабочей станции абонента, в частности IP-адреса, используемые для доступа в глобальной сети;

– мероприятия по обеспечению безопасности информации, проведенные при установке технических средств и программного обеспечения, е том числе средств защиты информации от НСД и от утечки по каналам ПЭМИН, антивирусных программ, наличие инструкции по обеспечению безопасности информации на АП.

При работе в Сети запрещается:

– подключать технические средства (серверы, рабочие станции), имеющие выход в глобальную сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к глобальной сети;

– изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;

– производить отправку данных без соответствующего разрешения;

– использовать носители информации с маркировкой: «Допускается использование только в Сети » на рабочих местах других систем (в том числе и персональных компьютерах) без соответствующей санкции.

Ведение учета абонентов, подключенных к глобальной сети, организуется в устанавливаемом в компании порядке.

Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на администраторов АП, руководителей соответствующих подразделений, определенных приказом руководителя компании, а также руководителя службы безопасности.

Лекцию разработал:

Доцент кафедры ИС

к.т.н., доцент

«___» _____20__ г. В.Е. Рачков