## АРХИВИРОВАНИЕ. ШИФРОВАНИЕ. КОНТРОЛЬ. АРХИТЕКТУРА

Архивирование информации, проходящей через технические каналы утечки:

Обязательной компонентой IPC является архив, который ведется для выбранных потоков информации (пакетов, сообщений). Вся информация о действиях сотрудников хранится в одной и нескольких связанных базах данных. Лидирующие IPC-системы позволяют архивировать все каналы утечки, которые они могут контролировать. В архиве IPC хранятся копии закачанных в интернет документов и текста, электронных писем, распечатанных документов и файлов, записанных на периферийные устройства. В любой момент администратор ИБ может получить доступ к любому документу или тексту в архиве, используя лингвистический поиск информации по единому архиву (или всем распределенным архивам единовременно). Любое письмо при необходимости можно посмотреть или переслать, а любой закачанный в Интернет, записанный на внешнее устройство или распечатанный файл или документ просмотреть или скопировать. Это позволяет проводить ретроспективный анализ возможных утечек и, в ряде случаев, соответствовать регулирующим деятельность документам, например, Стандарту Банка России *СТО БР ИББС-1.0-2008*.

Шифрование информации на всех точках сети:

Технология IPC включает в себя возможности по шифрованию информации на всех ключевых точках сети. Объектами защиты информации являются:

- Жесткие диски серверов,
- SAN,
- NAS,
- Магнитных лентах,
- Диски CD/DVD/Blue-ray,
- Персональные компьютеры (в том числе ноутбуки),
- Внешние устройства.

Технологии IPC используют различные подключаемые криптографические модули, в том числе наиболее эффективные алгоритмы DES, Triple DES, RC5, RC6, AES, XTS-AES. Наиболее используемыми алгоритмами в IPC-решениях являются RC5 и AES, эффективность которых можно проверить на проекте [distributed.net]. Они наиболее эффективны для решения задач шифрования данных больших объемов данных на серверных хранилищах и резервных копиях. В решениях IPC поддерживается интеграция с российским алгоритмом *ГОСТ 28147-89*, что позволяет применять модулей шифрования IPC в государственных организациях.

Контроль доступа к сети, приложениям и информации:

**Двухфакторная аутентификация** — это реализация контроля доступа, представляющая собой идентификацию пользователя на основе того, что он знает и того, чем он владеет.

Наиболее распространенная форма аутентификации часто — это обычные пароли, которые пользователь держит у себя в памяти. Пароли создают слабую защиту, так как они могут быть легко раскрыты или разгаданы (один из самых распространенных паролей — «password»). Политика безопасности, основанная на одних паролях, делает организацию уязвимой, поэтому в IPC применяется двухфакторная аутентификация с использованием распространенных USB-токенов.

Информационная сеть современных организаций гетерогенна в большинстве случаев. Это означает, что в одной сети совместно существуют сервера под управлением разных операционных систем и большое количество прикладных программ. В зависимости от рода деятельности предприятия, это могут быть приложения электронной почты и групповой работы, CRM-, ERP-, Sharepoint-системы, системы электронного документооборота, финансового и бухгалтерского учета и так далее. Количество паролей, которые необходимо помнить обычному пользователю, может в среднем по организации достигать от 3 до 7. Пользователи пишут

пароли на бумажках и приклеивают на видных местах, сводя тем самым на нет все усилия по защите информации, либо постоянно путают и забывают пароли, вызывая повышенную нагрузку на внутреннюю службу ИТ. Применение IPC в данном случае позволяет решить и вторичную задачу — упрощение жизни обычным сотрудникам совместно с повышением уровня защищенности.

На рисунке 1 представлена архитектура IPC-системы.

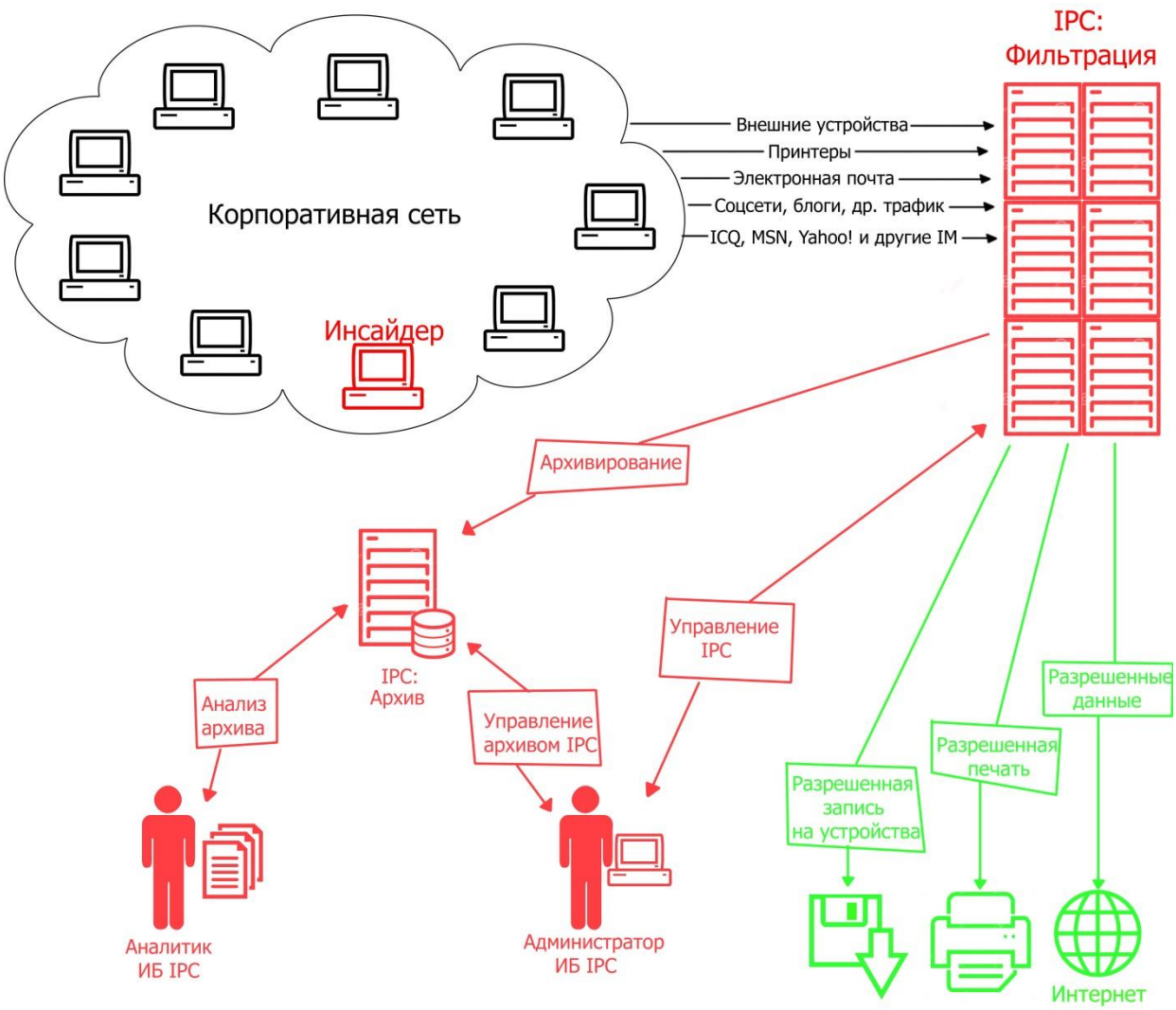


Рисунок 1 – «Диаграмма развертывания IPC-системы»

## БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦСЕТЯХ

В современном обществе невозможно обойтись без социальных сетей и в современном мире преобладают интернет технологии. В настоящее время

каждый человек, связанный с компьютером, зарегистрирован хотя бы в одной социальной сети. Социальные сети притягивают людей, так как в современном мире все люди общаются, обмениваются информацией, спамят, знакомится, большинство людей придумывают для себя виртуальный мир, в котором они могут быть бесстрашными, популярными посредством чего отказываются от реальности. Проблема, связанная с безопасностью персональных данных в социальных сетях является наиболее актуальной и интересной в современном социуме.

Многие не заботятся о безопасности персональных данных. Но почти любой сайт требует от нас ввода элементарной личной информации, как фамилии и имя, даты рождения. У большинства посетителей интернета пароль один и тот же на всех сайтах, что является плюсом для хакеров. Популярная атака является система онлайн-оплата услуг, где первым делом хакеры овладевают денежными ресурсами. Для этого создается фальшивый, поддельный, точный сайт, аналогичный существующему, на котором и происходят все махинации.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных[1].

Информационная безопасность становится ключевым фактором в процессе предоставления электронных услуг. Современные инфокоммуникационные услуги отличаются использованием большого объема чувствительной информации, которая нуждается в защите (персональные данные, платежная информация, ключи и секреты).

Меры безопасности в интернете:

1) Нельзя указывать личную информацию в социальных сетях (адрес проживания; домашний телефон) или делать её видимой только для друзей.

2) Своевременное обновление программного обеспечения.

3) Наличие на компьютере свежей версии антивирусной программы.

4) Игнорирование подозрительных сообщений.

5) Контакт-лист (список друзей) только с проверенными людьми.

6) Использование различных паролей для разных интернет-ресурсов.

7) Наличие на компьютере расширения (плагина) блокирующего всплывающие окна (например, AdBlock Plus).

Соблюдение этих мер ведет к снижению риска угроз со стороны мошенников.

Следует всегда помнить, что персональные данные каждого человека находятся под защитой Федерального закона РФ №152 «О защите персональных данных». Закон основывается на конфиденциальности персональных данных, целью является защита прав и свобод человека при обработке его персональных данных.

Влияние социальных сетей на нашу жизнь с каждым годом увеличивается и проникает во все сферы жизни. Например:

На экономическую:

Социальная сеть приносит прибыль тем людям, которые создают различные сайты, прибыль они получают благодаря популярности созданного сайта. Также в социальных сетях располагаются рекламные банера, приносящие прибыль. Реклама через социальную сеть более эффективна, так как больше людей ознакомятся с ней. По приблизительным оценкам, примерно 50% новостей мы узнаем из социальных сетей.

На социальную:

Современный мир-это мир информационных технологий, компьютеров и интернета. Виртуальное общение преобладает над реальными событиями, посредством виртуального мира человек лишается способности гармонично взаимодействовать с людьми в реальном времени.

На политическую:

Социальные сети являются эффективным инструментом для демократических преобразований .Если в обществе накопилось серьезное

недовольство, то собравшись в определенные группы в социальных сетях можно организовать митинг, по недовольству к власти, законам и др. Как показал опрос средний возраст участников группы составляет 20 лет, причем возраст 90% членов группы не превышает 25 лет.

В настоящее время для общения наиболее популярны такие сети, как: Vkontakte, Facebook, Google+, Socl. Я так же, как и большинство населения, пользуюсь социальными сетями. Для своего досуга и общения мне наиболее интересна социальная сеть Vkontakte и я хочу немного рассказать про эту сеть. Это популярная российская социальная сеть, основанная в 2006 году Павлом Дуровым выпускником филологического факультета Санкт-Петербургского государственного университета. Входит в тройку самых посещаемых сайтов Рунета. В прессе много обсуждали слухи о том, что Vkontakte финансируются или даже управляются ФСБ и управлением МВД. В пресс-службе социальной сети сотрудничества с правоохранительными органами не отрицали. По некоторым сведениям, именно благодаря доступу к переписке во Vkontakte и других социальных сетях, следователи выявили преступление в виде убийства[1].

Социальные сети приносят как вред, так и пользу их потребителям. Начнем с вреда, как уже оговаривалось, из-за социальных сетей многие люди перестали жить в реальности и больше погружаются в виртуальный мир. Меньше общаются с живыми людьми, именно поэтому многие люди становятся безграмотными, не владеют своей речью. Также следует отметить, что социальные сети отнимают много драгоценного времени. Во многих социальных сетях, существует раздел игры, которые также отнимают много и времени, но и еще некоторые игры требуют каких-либо денежных взносов, что соответственно влияет на бюджете потребителя. Игры в социальных сетях приносят пользу лишь их разработчикам. Польза социальных сетей, я считаю, заключается в том, что можно быстро, не затратив много времени обмениваться информацией. Можно бесплатно общаться с людьми из других стран и городов, что является огромным

плюсом, ведь если общаться с помощью писем, нужен длительный временной промежуток и некие денежные средства. Социальные сети очень разнообразны в своем применении, и каждый пользователь может выделить для себя положительные и отрицательные стороны. Анализируя свои действия человек, может научиться првильно и выгодно для себя обращаться с социальными сетями.

Защита персональных данных в социальных сетях является актуальной. Ведь при регистрации на каких-либо сайтах, требуют персональные данные каждого человека (ФИО, дата рождения и т.д.). Для защиты своих данных желательно регистрироваться только на проверенных сайтах (ведь сейчас много мошенников), также следует учитывать количество потребителей пользующихся той или иной сетью, не следует отправлять смс сообщения с различными кодами, придумывать сложные не однотипные пароли. При соблюдении этих правил о защите персональных данных, мне кажется, проблемы с взломом, повреждением сведутся до минимума. Главное всегда помнить о неразглашении своих данных на просторах сети Интернета.