ПОЛИТИКА ИБ СТРОЙБАНК

Компания АО «СТРОЙБАНК». Штат — 100 сотрудников. 5 руководство, 5 бухгалтерия, 50 — IT-отдел, 30 — менеджеры по работе с клиентами, 10 — отдел безопасности. Управление компании использует телефонную связь, MS Office и т. д. Бухгалтерия использует телефонную связь, MS Office, 1С: Бухгалтерию. IT-отдел разрабатывает комплексы систем по защите локальной сети организации от внешних и внутренних угроз, а также ее мониторинга. Обеспечивает функционирование сайта компании и личных кабинетов клиентов. Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи и др.

**Содержание**

[1. Общие положения и основные обязанности пользователя 1](#_Toc52881410)

[2. Обеспечение антивирусной безопасности 2](#_Toc52881411)

[3. Безопасность персональных данных 2](#_Toc52881412)

[4. Работа в сети Интернет 3](#_Toc52881413)

Общие положения включают перечисление нормативных документов, на основании которых создана политика безопасности, назначение документа, взгляды руководства Банка на обеспечение ИБ, на риски ИБ, нормативную базу для выполнения стратегии ЗИ, целевую аудиторию, взаимодействие с другими организациями и дочерними компаниями.

## Общие положения и основные обязанности пользователя

В этом разделе раскрываются основные понятия, используемые в документе, нормативно-правовые акты, на которые опирались разработчики, готовя документ, обязанности сотрудников по обеспечению безопасности. Обычно именно в этом разделе прописана ответственность за соблюдение норм регламента и за обеспечение сохранности конфиденциальной информации. Это крайне важно, так как работники, не уведомленные об обязанности по защите коммерческой тайны, конфиденциальной информации и иных сведений, имеющих особый режим доступа, могут передавать ее третьим лицам как намеренно, так и нет, оказавшись жертвой специалистов по социальной инженерии.

Требования информационной безопасности не могут быть выполнены, если работники не уведомлены о них под роспись.

Среди иных возможных обязанностей сотрудников компаний и работников IT-подразделений:

* исключать возможность доступа третьих лиц к документам, содержащим конфиденциальную информацию;
* не использовать чужие средства идентификации и не передавать никому свои, не входить в систему под чужим логином;
* соблюдать установленные уровни допуска к информации;
* не переписывать на съемные носители конфиденциальные данные без санкции руководителя, не передавать их по любым каналам связи, не раскрывать лицам, не имеющим соответствующего уровня доступа;
* соблюдать требования и правила по работе со средствами технической защиты, в том числе со средствами криптографической защиты;
* контролировать состояние автоматизированного рабочего места, сообщать СБ обо всех ситуациях, имеющих характер инцидентов информационной безопасности, а именно: нарушении целостности пломб, свидетельствующем о попытке проникнуть в охраняемую зону, некорректном срабатывании антивирусной защиты, нарушениях в работе программного обеспечения, выявленных изменениях файлов, выходе из строя периферийных устройств;
* обеспечивать отсутствие на своем АРМ самостоятельно установленных программ;
* исключать копирование любых файлов или текстовой информации в любых целях без получения санкции руководителя.

Этот перечень правил не является исчерпывающим. Часто в целях обеспечения информационной безопасности эти нормы выносят в отдельную инструкцию по работе с компьютерами и носителями информации, оставляя в регламенте только общие положения.

## Обеспечение антивирусной безопасности

Утечки информации благодаря целенаправленным хакерским атакам менее часты, чем ее хищение в целях осуществления конкурентной разведки, направленной на получение ценной информации о бизнесе компании. Но наиболее часто информация утрачивается, теряет целостность или попадает в руки третьих лиц благодаря действию вредоносных компьютерных программ – вирусов, троянов, логических бомб.

Поэтому целесообразно посвятить отдельный раздел регламента обеспечению антивирусной защиты.

В этом разделе необходимо рассмотреть:

* основные пути и способы попадания зараженной вирусом информации в систему компании;
* случаи, в которых пользователь вправе или обязан самостоятельно использовать антивирусную защиту и в которых он обязан сообщить об инциденте IT-подразделению, чтобы они могли принять решение в сфере своей компетенции;
* действия, которые запрещены пользователю при работе со средствами антивирусной защиты, в частности, ее отключение.

## Безопасность персональных данных

Если организация обрабатывает персональные данные сотрудников, клиентов или иных третьих лиц, нормативно-правовое регулирование такой обработки является достаточно строгим. Выделение в регламенте по обеспечению информационной безопасности специального раздела, с одной стороны, окажется дублированием Положение об обработке персональных данных, с другой стороны, еще раз напомнит пользователю о серьезности задачи по сохранению их конфиденциальности.

В разделе могут содержаться следующие положения:

* **основания доступа к информационным ресурсам и к обработке файлов**, содержащих персональные данные. Обычно таким основанием является включение сотрудника в перечень лиц, имеющих право работать с персональными данными. Обеспечение ограничения допуска облегчает контроль за сотрудниками, которые могут удалять, изменять или разглашать информацию;
* **обязанность работника изучать нормативно-правовые акты**, посвященные вопросам защиты персональных данных, а также направленные на решение этой задачи технические средства и регламенты;
* **действия, которые запрещены сотруднику**, допущенному к обработке ПД. Вносить изменения в конфигурацию компьютера или в программные продукты, обрабатывать персональные данные в присутствии третьих лиц, оставлять на рабочем месте документы или электронные носители информации, содержащие ПД, использовать ошибки в программах для распространения или изменения ПД;
* **меры ответственности**, применяемые к лицам, допущенным к обработке персональных данных и благодаря действиям которых произошло их разглашение.

## Работа в сети Интернет

Обеспечение информационной безопасности невозможно без соблюдения норм и правил по работе с Интернетом, электронной почтой, мессенджерами, иными каналами связи и передачи информации. В этом разделе устанавливаются разрешенные в компании способы использования Интернета, среди которых:

* ведение сайта компании;
* раскрытие информации о деятельности фирмы в случаях, предусмотренных федеральными законами;
* информационно-аналитическая работа;
* отправление почтовых сообщений. Чаще всего в компании устанавливают почтовый клиент, который позволяет отслеживать переписку.

В большинстве случаев и компаний иные способы использования Интернета должны согласовываться со службой безопасности или руководителем подразделения в целях обеспечения информационной безопасности. Некоторые компании формируют пакеты ресурсов Интернета, доступные пользователям в соответствии с их служебным статусом. Здесь же оговаривается применение средств антивирусной и иной технической защиты, обязанности по архивации почтового трафика, запрет на использование на рабочем месте ноутбуков или смартфонов с самостоятельным выходом в Сеть.