ООО «ПРОМГАЗНЕФТЬ»

Основные термины:

− администратор сети – сотрудник отдела информационных технологий, отвечающий за поддержание работоспособности локальной вычислительной сети и разграничение доступа к информационным ресурсам этой сети;

− безопасность информации - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.;

− доступ к информации – комплекс организационно-технических мероприятий, позволяющих сотруднику получить возможность ознакомления с информацией, в том числе с помощью технических средств, в соответствии с предоставленными ему для этого правами;

− защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

− защита информации от непреднамеренного воздействия - деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок её пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

− защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и(или) правил на изменение информации, приводящего к её искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

− защита информации от несанкционированного доступа – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами и собственником (Организация) прав или правил доступа к защищаемой информации;

− информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), используемые в целях принятия решений;

− информация Организации – информация, принадлежащая Организации, то есть: (а) созданная Организацией (его сотрудниками) в процессе его деятельности; (б) приобретенная Организацией на законных основаниях; (в) переданная Организацией его партнерами (клиентами) при установлении сотрудничества на правах совместного владения; (г) полученная в результате целенаправленного сбора информации подразделениями Организацией;

− информационная безопасность – состояние защищённости информационной среды, обеспечивающее минимизацию ущерба, вызванного возможной утечкой защищаемой информации, а также несанкционированных и непреднамеренных воздействий;

− информационная система – организационно-упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием вычислительной техники;

− информационная сфера (среда) - совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

− конфиденциальная информация – документированная информация, включенная в Перечень сведений, составляющих коммерческую тайну предприятия, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

− нарушение информационной безопасности – факт несанкционированного или непреднамеренного действия (операции) над информационной сферой, приводящий к нежелательным для предприятия последствиям;

− несанкционированный доступ – нарушение регламентированного доступа к объекту защиты;

− обработка информации – совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией;

− объект информатизации - совокупность информационных ресурсов, средств и систем обрабртки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для конфиденциальных переговоров;

− система защиты информации – совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации;

− средства связи – технические средства, используемые для формирования, обработки, передачи или приёма сообщений электросвязи либо почтовых отправлений;

− техническая защита информации – защита (не криптографическими методами) информации, содержащей сведения, составляющие государственную или коммерческую тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях её уничтожения, искажения и блокирования, и противодействие техническим средствам разведки;

− угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированным и/или непреднамеренным воздействиям на неё;

− утечка информации - неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками;

− шифрование – способ защиты информации, заключающийся в криптографическом преобразовании информации по специальному алгоритму для получения шифротекста и позволяющий предотвратить ее несанкционированное использование;

− цифровая подпись – дополнительные данные или криптографическое преобразование какого-либо блока данных, позволяющие получателю блока данных убедиться в подлинности отправителя и целостности блока данных и защитить его от искажения с помощью, например, средств получателя. Формы нарушения информационной безопасности:

а) пассивные − получение информации нарушителем для использования в своих целях;

− анализ характеристик информации без доступа к самой информации;

б) активные − изменение информации;

− внесение ложной информации − нарушение (разрушение) информации;

− нарушение работоспособности системы обработки информации.

Технический регламент:

* 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.

Инструкция к отделу управления по защите информации:

Управление по защите информации является основным методическим, координирующим и контрольным органом по вопросам информационной безопасности и исполняет эти функции в соответствии с Положением о Дирекции по безопасности и защите информации. В рамках этих функций Управление по защите информации:

* разрабатывает и проводит в жизнь концепцию обеспечения информационной безопасности ХХХХ;
* разрабатывает руководящие документы;
* разрабатывает методические документы;
* подготавливает для Члена Правления
* - Директора по безопасности и защите информации и принятия Правлением ХХХХ решения по вопросам информационной безопасности;
* организует и осуществляет взаимодействие с другими подразделениями ХХХХ, его дочерними зависимыми обществами (далее по тексту - ДЗО) и филиалов;
* взаимодействует с государственными органами и сторонними организациями;
* организует и совместно с подразделениями ХХХХ проводит первичное и контрольные информационные обследования;
* совместно с Управлением информационных систем и технологий и заинтересованными подразделениями разрабатывает требования и решения по защите информации для вновь принимаемых в эксплуатацию систем и средств информатизации;
* заказывает и закупает специальные средства защиты информации, контролирует и сопровождает их эксплуатацию после внедрения;
* контролирует эффективность принимаемых мер по обеспечению информационной безопасности, проводит общую оценку ее состояния;
* проводит плановые и внезапные проверки состояния информационной безопасности в подразделениях;
* консультирует и обучает сотрудников по вопросам информационной безопасности.