Приложение № 1 к Политике информационной
безопасности ПАО РОСНЕФТЬ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

Аутентификация пользователя – подтверждение того, что пользователь соответствует заявленному.

Безопасность информации (данных) – Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность (ГОСТ Р 53114-2008).

Безопасность информационной технологии – Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована (ГОСТ Р 53114-2008).

Блокирование информации (данных) – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе ее передачи.

Владелец информационного ресурса – работник или структурное подразделение, распоряжающийся информационным ресурсом, в том числе определяющий порядок доступа и его использования.

Вредоносная программа – программа, предназначенная для осуществления

несанкционированного доступа и (или) воздействия на информацию или ресурсы информационных систем.

Доступ к информации (данным) – возможность получения и использования информации (данных).

Защищаемая информация (защищаемые данные) – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (ГОСТ Р 53114-2008).

Идентификация риска – процесс обнаружения, распознавания и описания рисков (ГОСТ Р 53114-2008).

Информационная безопасность – состояние защищенности интересов организации в условиях угроз в информационной сфере. (ГОСТ Р 53114-2008).

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам (по ГОСТ Р 53114-2008).

Информационные процессы – процессы создания, сбора, обработки, накопления, хранения, поиска, передачи и уничтожения информации.

Информационные ресурсы – документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Информационная система – система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы и методы создания, поиска, сбора, хранения, обработки, предоставления, распространения информации и

способы осуществления таких процессов и методов.

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (по ГОСТ Р 53114-2008).

Источник угрозы безопасности – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации (данных) – обязательное для соблюдения требование не допускать распространения информации без согласия владельца информации или наличия иного законного основания.

Конфиденциальная информация (данные, сведения): документированная информация, доступ к которой ограничивается в соответствии с законодательством.

Корпоративная информационная система – общая распределенная информационная система, используемая для автоматизации процессов обработки информации и управления, реализуемая средствами информационных технологий и организационными мерами.

Управление ИБ– скоординированные действия по руководству и управлению в части обеспечения информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды (по ГОСТ Р 53114-2008).

Управление рисками ИБ–скоординированные действия по руководству и управлению в отношении рисков ИБ с целью их минимизации (по ГОСТ Р 53114-2008).

Меры обеспечения ИБ – совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

Мониторинг ИБ – Непрерывное наблюдение за состоянием и поведением объектов ИБ с целью их контроля, оценки и прогноза в рамках управления ИБ.

Нарушитель ИБ – физическое лицо, случайно или преднамеренно

совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации (данных) – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обеспечение ИБ– деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности или на минимизацию ущерба от возможной реализации таких угроз (ГОСТ Р 53114-2008).

Обработка информации (данных) – действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение информации.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты информации – информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 53114-2008).

Объект ИБ – компонент информационной сферы, на который направлена деятельность по обеспечению ИБ.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии заданной информационной технологией, а также средств их обеспечения,

помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены (ГОСТ Р 53114-2008).

Оценка риска – процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку (ГОСТ Р 53114-2008).

Политика – общее намерение и направление, официально выраженное руководством (ГОСТ Р ИСО/МЭК 27002-2012).

Система управления информационной безопасностью (СУИБ) – часть общей системы управления Институтом, основанная на использовании методов оценки рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности (по ГОСТ Р 53114-2008).

Система обеспечения информационной безопасности – совокупность нормативно-правовых, организационных и технических мер по обеспечению защищенности интересов в информационной сфере, а также субъектов информационных отношений.

Технические средства информационных систем – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации, применяемые в информационных системах.

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное воздействие – несанкционированное воздействие на

ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение информации (данных) – действия, направленные на передачу информации определенному кругу лиц или на ознакомление с информацией неограниченного круга лиц, в том числе обнародование в средствах массовой информации, размещение в информационно телекоммуникационных сетях или предоставление доступа к информации каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Риск – сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2012).

Роль ИБ – совокупность прав, привилегий и ограничений на использование ресурсов корпоративной информационной системы, предоставляемая работникам и третьим лицам для выполнения ими функциональных обязанностей.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Система защиты информации (данных) – совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения блокирования, копирования, распространения, а также иных неправомерных действий с ней.

Третья сторона – лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме (ГОСТ Р ИСО/МЭК 27002-2012).

Угрозы безопасности информации (данных) – совокупность условий и

факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать ее уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при ее обработке в информационных системах.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации (данных) – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях ее случайного и (или) преднамеренного искажения (разрушения).