Приложение № 1к Политике информационной безопасности ООО "ЦИФРОВАЯ НЕЗАВИСИМОСТЬ"

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.

Аутентификация – процедура проверки подлинности, которая включает в себя проверку принадлежности субъекту прав доступа к информационным ресурсам системы или веб-сайта в соответствии с предъявленным им идентификатором, а также подтверждение подлинности субъекта.

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

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.

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

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.

Идентификация риска – процесс обнаружения, распознавания и описания рисков.

Информационная безопасность – защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

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.

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

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством. К конфиденциальным относятся сведения:

а) о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);

б) составляющие тайну следствия и судопроизводства;

в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

г) связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

д) связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

е) о сущности изобретения, исследования, разработки, модели или промышленного образца до официальной публикации информации о них.

Управление ИБ – это совокупность мероприятий, направленных на обеспечение конфиденциальности, целостности и доступности информации, а также на минимизацию рисков кибербезопасности.

Управление рисками ИБ – это процесс, включающий в себя определение, оценку и управление рисками, связанными с безопасностью информационных ресурсов.

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 её 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 – это комплекс мероприятий, направленных на обеспечение конфиденциальности, целостности и доступности информации, а также на минимизацию рисков кибербезопасности.

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 защиты информации – информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации.

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

помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены.

Оценка риска – процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку.

Политика – общее намерение и направление, официально выраженное руководством.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления Организации, основанная на использовании методов оценки рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

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

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.

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

Риск – сочетание вероятности события и его последствий. Применительно к ИБ, риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

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.

Угрозы безопасности информации (данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать еѐ уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при еѐ обработке в информационных системах.

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