Приложение № 1к Политике информационной безопасности Банк ПАО ВТБ

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 – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности

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) - это процесс применения специальных мер и механизмов с целью ограничения доступа к определенной информации или данным. Этот процесс используется для обеспечения безопасности и конфиденциальности информации, а также для предотвращения несанкционированного доступа или использования данных.

Вредоносная программа - это программы, намеренно разработанные и внедряемые для нанесения ущерба компьютерам и компьютерным системам. (

определение взято с сайта https://www.kaspersky.ru/resource-center/threats/types-of-malware)

Доступ к информации (данным) - это возможность получения, использования и просмотра информации, которая хранится в информационной системе, базе данных, документах или других источниках. Доступ к данным может быть ограничен или разрешен в зависимости от различных факторов, таких как уровень аутентификации и авторизации, политики безопасности, правила доступа и т. д.

Защищаемая информация (защищаемые данные) - это категория информации, которая требует особой заботы, мер безопасности и контроля доступа из-за своей важности, конфиденциальности, ценности или рисков, связанных с её разглашением или утратой.

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

Идентификация риска - процесс обнаружения, распознавания и 12 описания рисков (ГОСТ Р 53114-2008).

Информационная безопасность – защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность (ГОСТ Р ИСО/МЭК 27002-2012)

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

Информационные ресурсы - совокупность всей информации, накопленной человечеством в процессе развития науки, культуры, образования и практической деятельности людей

Информационная система - это комплексный набор компонентов, включающих в себя программное обеспечение, аппаратное оборудование,

данные, процедуры и людей, которые работают вместе для сбора, обработки, хранения, передачи и использования информации с целью поддержки операций и принятия решений в организации или в другом контексте.

Информационные технологии - процессы, использующие совокупность средств и методов сбора, обработки, накопления и передачи данных для получения информации нового качества о состоянии объекта, процесса, явления, информационного продукта, а также распространения информации и способы осуществления таких процессов и методов.

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

Источник угрозы безопасности - это фактор, организация, или событие, которые могут создавать риски и угрозы для безопасности информации, систем или ресурсов.

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Управление ИБ - это набор политик, инструментов и процедур, используемых для защиты корпоративной информации и данных от угроз и атак. (ГОСТ Р 53114-2008)

Управление рисками ИБ - представляет собой непрерывный процесс, обеспечивающий выявление, оценку и минимизацию рисков от реализации угроз информационной безопасности, направленных на активы организации. (ГОСТ Р 53114-2008).

Меры обеспечения ИБ - это набор действий, политик, процедур, технологий и практик, применяемых для защиты информации и информационных систем от угроз, рисков и потенциальных нарушений 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 (субъект), случайно или преднамеренно совершившее 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, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональному предназначению и техническим характеристикам.

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) - это процесс преобразования входных данных в полезную информацию путем выполнения различных операций и действий с этими данными.

Объект защиты информации - это конкретный ресурс, элемент или аспект, который подлежит защите в контексте информационной безопасности.

Объект информатизации - средства электронной вычислительной техники вместе с программным обеспечением, в том числе системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или)

технологическими процессами.

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

Обработка риска - процесс выбора и реализации мер по модификации (снижению) риска.

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

Система управления информационной безопасностью (СУИБ) - часть общей системы управления, 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 органов, методов (способов), сил и средств обеспечения информационной безопасности.

Пользователь информационной системы - это человек, который взаимодействует с информационной системой (ИС) или использует её для выполнения определённых задач, получения информации или достижения своих целей.

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

Ресурс информационной системы - это любой элемент, компонент или средство, используемое для функционирования и поддержания информационной системы (ИС).

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

Средства вычислительной техники - это оборудование и устройства, используемые для выполнения вычислений и обработки данных.

Субъект доступа - пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются

правилами разграничения доступа.

Система защиты информации (данных) - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая в соответствии с требованиями о защите информации.

Угрозы безопасности информации (данных) - это потенциальные события, действия, ситуации или условия, которые могут вызвать ущерб, нарушение конфиденциальности, целостности или доступности информации или данных.

Уязвимость - это слабое место, дефект, недостаток или недоразумение в системе, программном обеспечении, аппаратуре или процессе, которое может быть использовано злоумышленниками или вызвать ошибки, что, в свою очередь, может привести к угрозам безопасности или ненадежности системы.

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.