Приложение № 2 к Политике информационной безопасности {БАНК ПАО ЗЕНИТ}

ПОЛОЖЕНИЕ
О РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИБ

1. Назначение и область действия

1.1 Настоящее Положение о порядке выявления и реагирования на инциденты информационной безопасности (далее - Положение) устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы персональных данных Банка ПАО Зенит (далее - Банк) и (или) возникновению угроз безопасности конфиденциальной информации Банка (далее - инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима служебной тайны (далее - служебное расследование) в Банке.

1.2 Настоящее Положение распространяется на сотрудников Банка.

1.3 Процесс управления инцидентами ИБ включает:

– учет и регистрацию инцидентов ИБ;

– оповещение ответственного лица о возникновении инцидентов ИБ;

– расследование обнаруженных инцидентов ИБ;

– устранение причин и последствий инцидентов ИБ;

– определение плана корректирующих и превентивных мероприятий.

1.4. Требования настоящего Положения являются обязательными для выполнения всеми сотрудниками Банка.

2. Основные требования

2.1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности

операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем Банка.

2.2. В обязательном порядке должны регистрироваться следующие события безопасности:

– попытки входа (выхода) пользователей в операционную систему (из операционной системы);

– загрузка и инициализация операционной системы рабочих станций и серверов;

– попытка доступа к средствам виртуализации;

– факт изменения конфигурации средств виртуализации;

- запуск и остановка служб (системных сервисов) средств виртуализации;

- попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.3. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

– тип события;

– дата и время события;

– результат события;

– источник события;

- идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.4. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.5. Учет инцидентов ИБ осуществляется работниками службы по противодействию угроз информационной безопасности, назначенными приказом Банка. Допускается ведение учета инцидентов ИБ как в бумажном виде, так и в электронном виде.

2.6. При обнаружении инцидента ИБ администратор информационной безопасности проводит его классификацию в соответствии с Приложением к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

3. Роли и ответственность

3.1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный по защите информации.

3.2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет руководитель службы по противодействию угроз информационной безопасности.