softline®
Мы всё сможем
30 лет в ИТ

Трансформация.
Успешная. Цифровая. Защищенная.

Выполнение требований ЦБ.

ГОСТ 57580, риски и операционная надежность

Юлия Задубровская

Руководитель направления
безопасности финансовых операций

ГК Softline

Трансформация.
Успешная. Цифровая. Защищенная.

Infosecurity

специализированный сервис-провайдер,
уже более 10 лет оказывающий услуги в сфере

- информационной безопасности
- IT и консалтинга
- лицензиат ФСБ России и ФСТЭК России

Компания успешно внедряет и сопровождает системы защиты информации в различных отраслях:

- финансы
- промышленность
- медицина
- государственный сектор

и др.

Специализация

- Техническая поддержка
- Внедрение
- Compliance
- Аналитическая поддержка
- Безопасность как сервис (MSSP)
- Аудит
- Проектирование
- Консалтинг
- Обучение

>25 000
угроз выявляем ежемесячно

>250
профессионалов в команде

>20
сервисов и услуг для защиты бизнеса

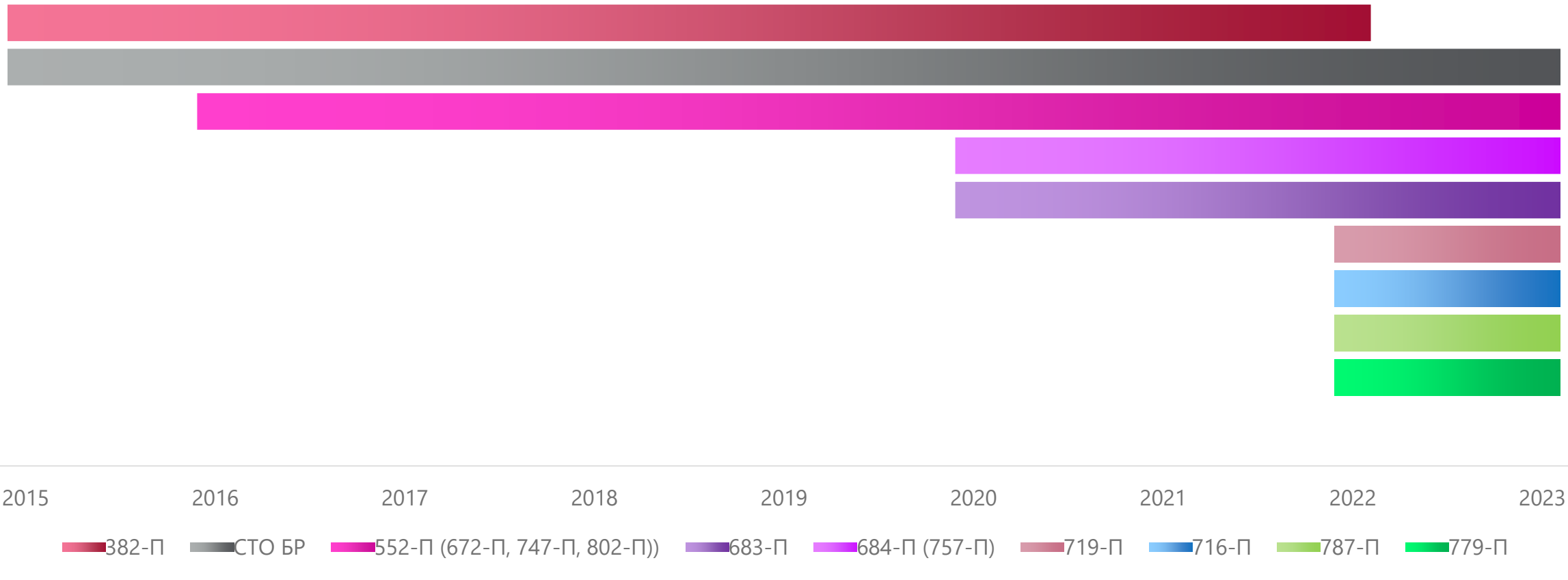
>350
компаний под нашей защитой

Мы всё сможем

softline® 30 лет в ИТ

Нормативные документы ЦБ РФ

История требований к защите информации



Комплексный подход ЦБ к безопасности

Комплексный подход ЦБ к безопасности

Система управления рисками

Система управления рисками

Планирование

- ОРД, определяющие процедуры управления рисками
- Ответственные работники, подразделения-участники
- Порядок взаимодействия подразделений в рамках управления рисками
- Функции и полномочия участников процедур управления рисками
- Риск-аппетита организации
- КПУР
- Порядок мониторинга показателей уровня риска
- Порядок выявления и обработки событий риска
- Порядок контроля эффективности процедур управления рисками
- Порядок совершенствования системы управления рисками
- Порядок участия руководства в процессах управления рисками
- Порядок, способ и формы внутренней отчетности
- Возможные источники угроз и рисков, сценарии реализации, моделирование угроз
- Методика оценки риска
- Порядок кадрового обеспечения и требования к персоналу

Система управления рисками

Реализация

- Критичные бизнес-и технологических процессы
- Способ реагирования на выявленные риски
- КПУР с учетом риск-аппетита компании
- Плана реагирования на риск
- Мониторинг, выявление и обработка выявленных рисков
- Ведение базы событий рисков
- Способ и порядок возмещения потерь от реализации рисков
- Состав, содержание, исполнение организационных и технических мер защиты информации (включая меры защиты ГОСТ 57580.1-2017)
- Состав, содержание, исполнение организационных и технических мер обеспечения операционной надежности (включая меры защиты ГОСТ 57580.4-2022)
- Процессы, передаваемые на аутсорсинг
- Управление риском использования аутсорсинга
- Требований к процедурам снижения рисков для контрагентов
- Повышение осведомленности работников и контрагентов

Система управления рисками

Контроль

- Периодическая оценка выполнения требований к защите информации (включая ГОСТ 57580.1-2017)
- Периодическая оценка выполнения требований к операционной надежности
- Периодическая оценка эффективности системы управления рисками
- Оценка фактических значений КПУР
- Определение КИР и порядка их расчета, мониторинг значений КИР
- Определение правил привлечения проверяющих организаций и требования к ним
- Фиксация оценок, как внешних, так и внутренних
- Внутренняя отчетность по итогам контрольных мероприятий и выполненных процедур управления риском, защиты информации, управления операционной надежностью
- Информирование руководства о результатах оценок
- Информирование регуляторов (информационные сообщения, отчетность)

Система управления рисками

Совершенствование

- Решение о необходимости совершенствования системы управления рисками
- Пересмотр сигнальных и контрольных значений КПУР
- Пересмотр риск-аппетита
- Пересмотр достаточности и порядка выполнения применяемых мер защиты
- Пересмотр состава применяемых технологий
- Пересмотр кадровой политики
- Пересмотр технологических процессов
- Пересмотр политики использования аутсорсинга
- Решение об изменении документов, процессов, мер защиты на основе изменения законодательства, изменения внутренних процессах, реализовавшихся инцидентах и рисках, результатов контрольных мероприятий и оценок, включая оценку рисков
- Доведение до руководства результатов анализа эффективности системы управления рисками, принятие руководством решения о необходимых мероприятиях по ее совершенствованию
- Контроль со стороны руководства за реализацией планов совершенствования

КПУР ИБ

Финансовые и бизнес-показатели

- Величина потерь от реализации событий риска ИБ и доля от базового капитала (отдельно – по событиям, связанным с переводами денежных средств)
- Доля переводов денежных средств без согласия клиента
- Доля денежных средств по операциям без согласия клиента
- Объем капитала, который организация готова выделить для покрытия ущерба от рисков ИБ
- Доля заблокированных банком операций клиентов
- Доля возмещенных клиентам денежных средств

КПУР ИБ

Показатели выполнения требований к ЗИ

- Доля событий риска ИБ, отраженных в базе событий
- Доля событий риска ИБ, о которых проинформирован Банк России
- Оценка уровня соответствия Процесса 1 ГОСТ 57580.1-2017
- Оценка уровня соответствия Процесса 5 ГОСТ 57580.1-2017
- Оценка уровня соответствия ГОСТ 57580.1-2017 в целом
- Оценка выполнения иных требований регуляторов
- Оценка по направлению «оценка эффективности функционирования системы управления риском информационной безопасности», проведенная уполномоченным подразделением и (или) внешним экспертом

ГОСТ 57580.3-2022

Уточнение и дополнение требований Положения № 716-П

- Процедуры управления риском;
- Определение во внутренних документах политики управления риском;
- Мониторинг, выявление и классификация событий риска, а также реагирование на них;
- Определение и мониторинг КИР и КПУР;
- Оценка риска;
- Ведение базы событий риска;
- Отчетность в рамках управления риском и информирование заинтересованных лиц и организаций;
- Оценка эффективности системы управления риском;
- Распределение функций подразделений по управлению риском

ГОСТ 57580.3-2022

Новые особенности процесса управления риском реализации информационных угроз

- Принцип «трех линий защиты»;
- Расширенная классификация событий риска;
- Увеличение КПУР с делением по группам;
- Больше требований к оценке СВР событий риска и СТП;
- Больше требований к оценке риска, связанного с недостатками кадрового обеспечения;
- Требования к квалификации работников службы ИБ;
- Больше внутренней отчетности для всех подразделений, связанных с управлением риском;
- Больше информирования и привлечения руководства к деятельности по управлению риском;
- Больше процедур по управлению риском при привлечении поставщиков услуг

Отчетность в части управления рисками

Кредитные организации

Отчетность по управлению рисками

- Отчетная форма 0409106

Отчетность о выполнении ГОСТ 57580.3-2022

- На данный момент отсутствует

Некредитные организации

Отчетность по управлению рисками

- Отчетная форма 0420720 (только для операторов инвестиционной платформы, финансовой платформы, ИС, в которых осуществляется выпуск ЦФА, операторов обмена ЦФА)

Отчетность о выполнении ГОСТ 57580.3-2022

- На данный момент отсутствует

Обеспечение операционной надежности

ГОСТ 57580.4-2022

Уточнение и дополнение требований Положения № 787-П/ 779-П

- Определение в ВНД порядка управления ОН;
- Идентификация и учет элементов критичной архитектуры;
- Тестирование ОН;
- Управление изменениями критичной архитектуры;
- Выявление, регистрация инцидентов ОН, реагирование на них, а также восстановление выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации таких инцидентов;
- Управление доступом, включая удаленный доступ;
- Взаимодействие с поставщиками услуг в сфере информационных технологий;
- Обеспечение осведомленности об актуальных информационных угрозах и их нейтрализация

ГОСТ 57580.4-2022

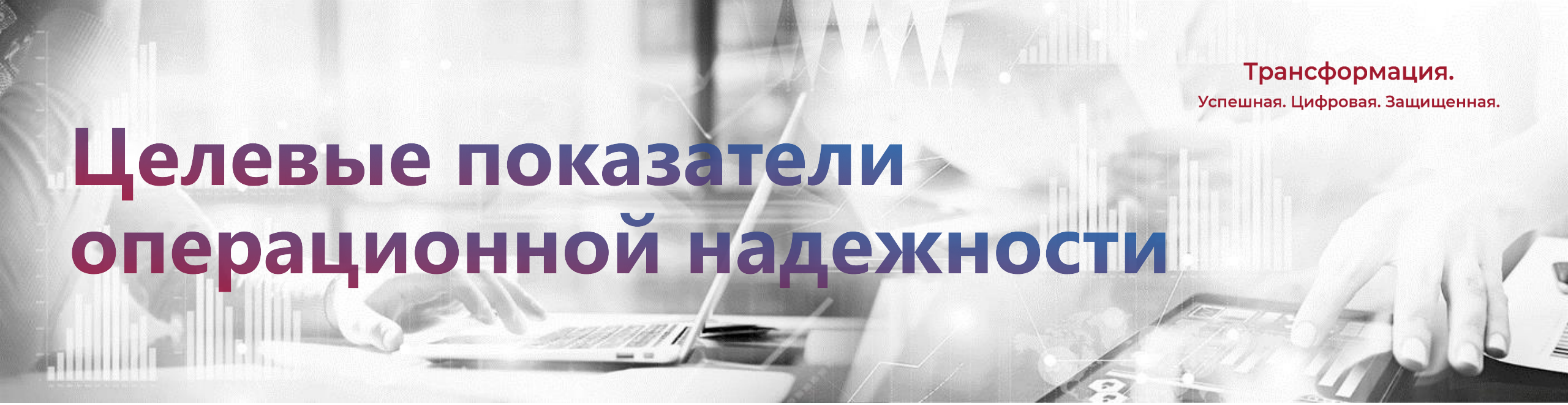
Новые требования к процессу обеспечения ОН

- Контрольные и сигнальные значения КПУР;
- Доведение фактических значений части КПУР до клиентов;
- Больше требований к идентификации, учету и контролю состава элементов критичной архитектуры, включая их классификацию;
- Больше требований к управлению изменениями элементов критичной архитектуры;
- Разработка стандартов конфигурирования технических средств и систем, относящихся к критичной архитектуре, их согласование службой ИБ и контроль их изменения;
- Больше требований к выявлению, регистрации инцидентов ОН и реагированию на них;
- Больше требований к восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации таких инцидентов

ГОСТ 57580.4-2022

Новые требования к процессу обеспечения ОН

- Оценка эффективности деятельности по выявлению, реагированию на инциденты и восстановлению в рамках регулярной оценки эффективности системы управления риском реализации информационных угроз;
- Больше внутренней отчетности в рамках управления ОН и риском реализации информационных угроз;
- Больше информирования и привлечения руководства к деятельности по управлению ОН;
- Больше процедур по управлению безопасности цепи поставок для управления ОН при привлечении поставщиков услуг
- Больше мер по обеспечению безопасности при удаленном доступе, включая доступ для технического обслуживания и диагностики элементов критичной архитектуры



Целевые показатели операционной надежности

- Допустимая доля деградации технологического процесса (ДДД);
- Допустимое время простоя и (или) деградации технологического процесса в рамках инцидента операционной надежности (ДВП/ДВД);
- Допустимое суммарное время простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение очередного календарного года (ДСВ);
- Показатель соблюдения режима работы (функционирования) технологического процесса

Методики расчета ДДД

Установление контрольного значения ДДД=1

- Плюсы
  - Признание инцидентом ОН при любом отклонении фактической ДД от 1
  - Отсутствие необходимости расчетов фактической ДД
- Минусы
  - Любой сбой признается инцидентом
  - Очень большое количество уведомлений в ЦБ РФ
  - Низкие показатели операционной устойчивости в отчетности

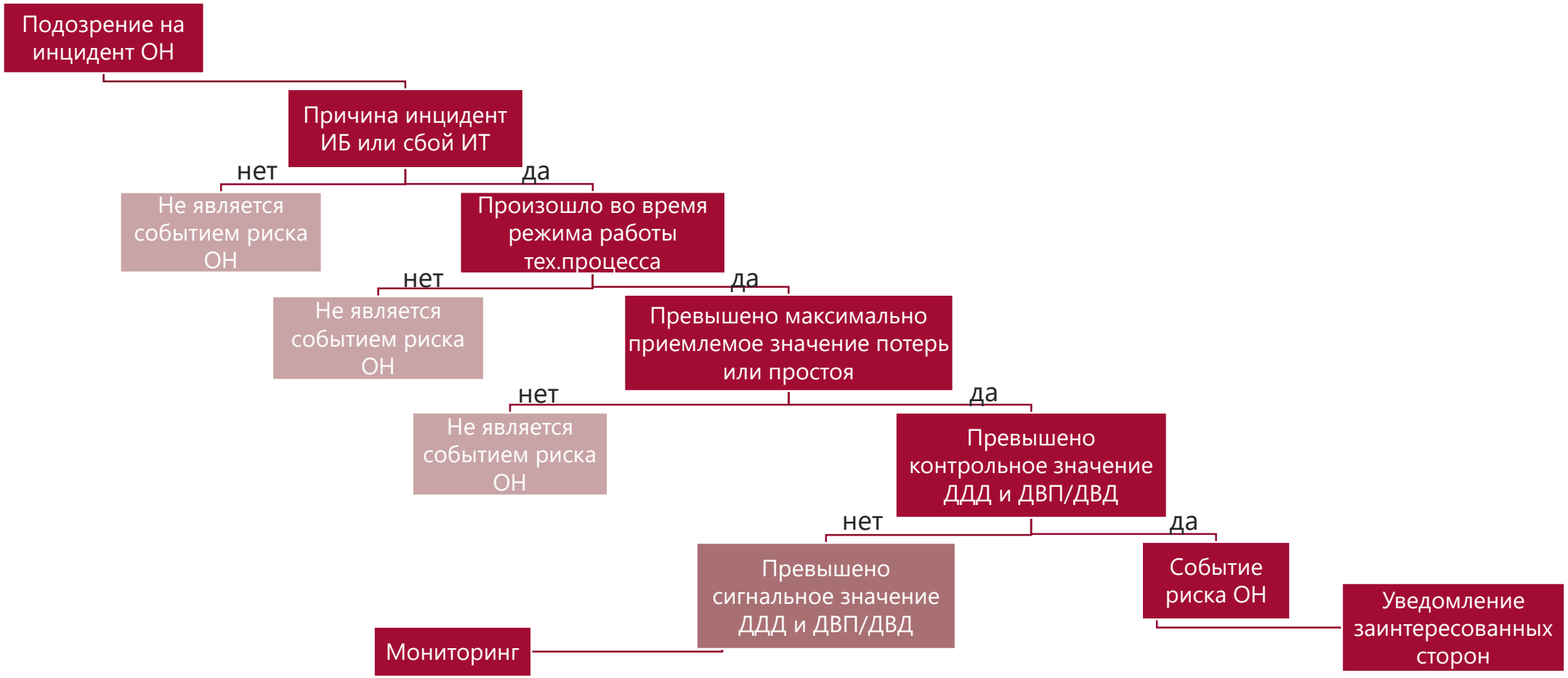
Распространение ДД процедуры на техпроцесс

- Плюсы
  - Упрощение расчетов фактической ДД, т.к. достаточно расчетов ДД пострадавшей процедуры
- Минусы
  - Большое количество уведомлений в ЦБ РФ
  - Средние показатели операционной устойчивости в отчетности

Расчет фактической ДД аналогично ДДД

- Плюсы
  - Высокая точность и дифференцированность анализа фактической ДД
  - Небольшое количество уведомлений в ЦБ РФ
  - Высокие показатели операционной устойчивости в отчетности
- Минусы
  - Сложность и трудоемкость расчетов

Определение инцидента операционной надежности



Отчетность по операционной надежности

Кредитные организации

Отчетность по управлению операционной надежностью

- Отчетная форма 0409072 (проект указания Банка России на утверждении)

Отчетность о выполнении ГОСТ 57580.4-2022

- На данный момент отсутствует

Некредитные организации

Отчетность по управлению операционной надежностью

- Отчетная форма 0420174 (страховые компании);
- Отчетная форма 0420432 (участники рынка ценных бумаг, организаторы торговли, клиринговые организации);
- Отчетная форма 0420265 (НПФ);
- Отчетная форма 0420721 (операторы инвестиционной платформы, финансовой платформы, ИС, в которых осуществляется выпуск ЦФА, операторы обмена ЦФА);
- Отчетная форма 0420523 (управляющие компании фондов, инвестиционные фонды)

Отчетность о выполнении ГОСТ 57580.4-2022

- На данный момент отсутствует

Обеспечение защиты информации

Выполнение требований по защите информации

Определение требований	• Нормативный документ в зависимости от типа организации и вида деятельности • Применяемые требования документа
Определение области действия требований	• Технологические и бизнес-процессы • Информационные системы
Определение применяемых мер защиты	• Адаптация базового набора мер на основе применяемых технологий, результатов проведения моделирования угроз и оценки рисков
Регламентация	• Закрепление в ВНД области действия требований, ответственных, участников • Определение содержания и состава применяемых мер
Реализация	• Внедрение/модернизация процессов и организационных мер • Внедрение/настройка/модернизация ИС и СЗИ
Контроль и совершенствование	• Проведение регулярных контролей, внешних и внутренних оценок • Периодический пересмотр состава мер защиты и порядка их реализации

Отчетность по защите информации

Кредитные организации

Отчетность по уровню защиты информации

- Отчетная форма 0409071

Отчетность о выполнении ГОСТ 57580.1-2017

- Отчетная форма 0409071

Некредитные организации

Отчетность по уровню защиты информации

- Отчетная форма 0420175 (страховые компании);
- Отчетная форма 0420433 (участники рынка ценных бумаг, организаторы торговли, клиринговые организации);
- Отчетная форма 0420266 (НПФ);
- Отчетная форма 0420722 (операторы инвестиционной платформы, финансовой платформы, ИС, в которых осуществляется выпуск ЦФА, операторы обмена ЦФА)

Отчетность о выполнении ГОСТ 57580.1-2017

- Аналогично формам выше

Трансформация.
Успешная. Цифровая. Защищенная.

Юлия Задубровская

Руководитель направления
безопасности финансовых организаций

INFOSECURITY
a Softline company

Sergey.Senyutin@softline.com

Мы всё сможем

softline 30 лет в ИТ


softline®
Мы всё сможем
30
лет в ИТ
Трансформация.
Успешная. Цифровая. Защищенная.