КОД БЕЗОПАСНОСТИ

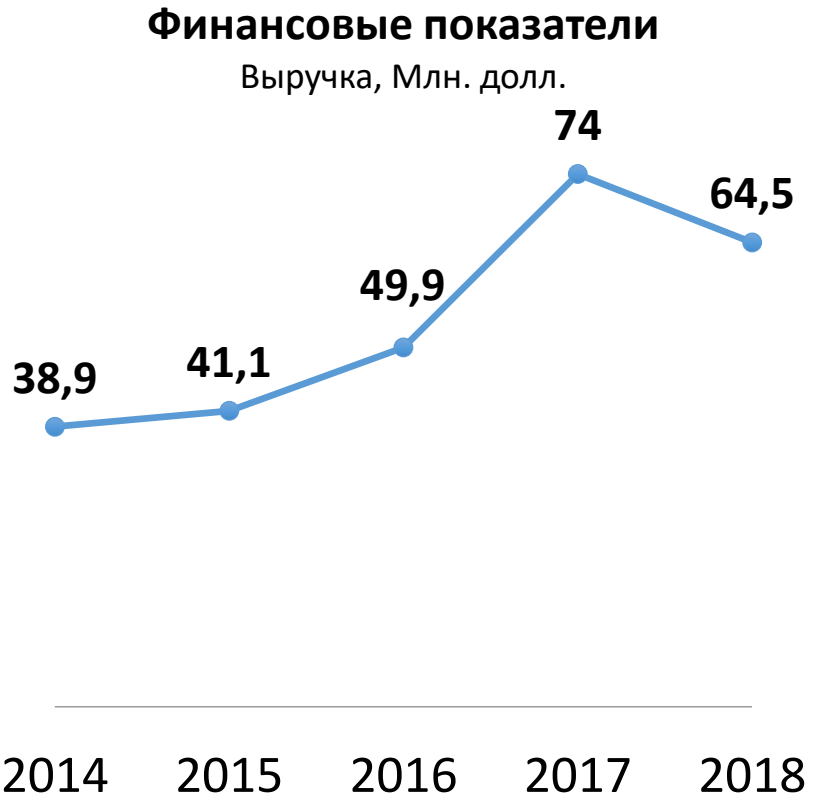
Положения 683-П и 684-П: Новые требования к информационной безопасности финансовых организаций

Павел Коростелев, 01.11.2019

КОД БЕЗОПАСНОСТИ

Коротко о «Коде безопасности»

- **Разработчик** средств информационной безопасности
- Образован в **1995**
- Штаб квартира в **Москве**
- Международный офис в **Дубае**
- 500 разработчиков в трех городах:
  - Москва
  - Санкт-Петербург
  - Пенза
- **32 000** заказчиков & **1.5M** защищенных рабочих мест



Самое важное

1. ЦБ утвердил требования к защите информации в электронных документах составленных при осуществлении **любых** банковских операций
2. Область действий требований значительно шире, чем раньше (ПС БР, ЕБС и тд)
3. Для некредитных организаций раньше ничего сопоставимого не было!
4. Контроль соответствия требованиям проходит в форме **внешнего аудита**
5. Аудит проводится **раз в два года**

Самое важное

1. ЦБ утвердил требования к защите информации в электронных документах составленных при осуществлении **любых** банковских операций
2. Область действий требований значительно шире, чем раньше (ПС БР, ЕБС и тд)
3. Для некредитных организаций раньше ничего сопоставимого не было!
4. Контроль соответствия требованиям проходит в форме **внешнего аудита**
5. Аудит проводится **раз в два года**

Требования уже начали действовать!

КОД БЕЗОПАСНОСТИ

Ключевые элементы новых положений

Защита ИТ-инфраструктуры в соответствии с ГОСТ 57580

Контроль защищенности инфраструктуры

Контроль защищенности платежных приложений

Управление инцидентами ИБ

Выполнение требований работы с СКЗИ

Выполнение требований безопасности к технологиям обработки информации

КОД БЕЗОПАСНОСТИ

Что защищаем?

- Электронные документы созданные при осуществлении финансовых операций
- Информация для авторизации клиентов для осуществления финансовых операций
- Информация о финансовых операциях
- Информация о ключах шифрования используемых при осуществлении финансовых операций

Обзор ГОСТ 57580

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

Изменения в подходе регулятора

Все-в-одном

- СТО БР
- 382-П

Ссылки на унифицированный набор требований

- Приказ Минкомсвязи №321 (Защита ЕБС)
- Положение 672-П (Защита информации ПС БР)
- Положение 683-П
- Универсальный список мер защиты (ГОСТ 57580.1-2017)
- Методика оценки соответствия (ГОСТ 57580.2-2018)

А что для некредитных финансовых организаций?

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

Кого заденет положение 684-П?

- **Страховые организации**
  - В течении второго полугодия предыдущего года стоимость активов превышала 20 млрд. руб.
- **Негосударственные пенсионные фонды**
  - Обеспечивается обязательное пенсионное страхование
  - В рамках негосударственного пенсионного обеспечения размер пенсионных резервов в течении второго полугодия предыдущего года превышал 10 млрд. руб.
- **Брокеры**
  - С 2-го по 4-й кварталы предыдущего года обслуживали более 100 тыс. физических и юридических лиц
  - С 2-го по 4-й кварталы предыдущего года от лица клиентов совершено операций на 100 млрд руб ежеквартально
- **Депозитарии**
  - Центральный депозитарий
  - Депозитарий, который с 2-го по 4-й кварталы предыдущего года осуществлял учет ценных бумаг стоимостью более 500 млрд. Руб
  - Спецдепозитарии инвестиционных фондов, ПИФов и НПФов
- **Центральные контрагенты**
- **Дилеры**
  - С 2-го по 4-й кварталы предыдущего года за свой счет совершено операций на 200 млрд руб ежеквартально

КОД БЕЗОПАСНОСТИ

Кого заденет положение 684-П? (2)

- **Управляющие**
  - С 2-го по 4-й кварталы предыдущего года в рамках управления совершено операций на 20 млрд руб
  - С 2-го по 4-й кварталы предыдущего года осуществлялось доверительное управление в интересах более 2000 физических и юридических лиц
- **Регистраторы**
  - С 2-го по 4-й кварталы предыдущего года были открыты лицевые счета более 1 000 000 физических и юридических лиц
- **Репозитарии**
- **Клиринговые организации**
- **Организаторы торговли**

КОД БЕЗОПАСНОСТИ

Уровни защиты

Уровень защиты информации	Сопоставимый уровень защищенности персональных данных	
1 - Усиленный	УЗ-1	Системно значимые банки Центральный депозитарий Центральные контрагенты
2 – Стандартный	УЗ-2, УЗ-3	Все остальные банки и НФО, удовлетворяющие требованиям
3 – Минимальный	УЗ-4	----

КОД БЕЗОПАСНОСТИ

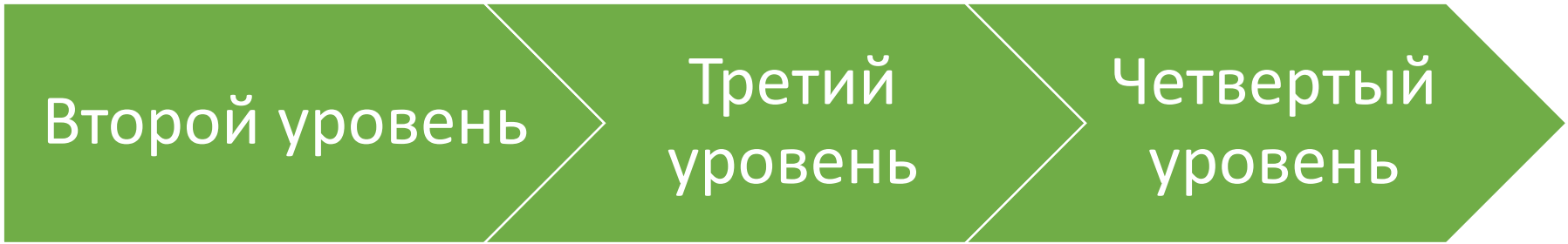
Уровни соответствия ГОСТ для банков

Уровень соответствия	Диапазон значений	
Нулевой	0	Все очень плохо…
Первый	До 0,5	Меры системы защиты реализуются бессистемно
Второй	От 0,5 до 0,7 (включительно)	Меры осуществляются в значительном объеме
Третий	От 0,7 до 0,85 (включительно)	Меры осуществляются в значительном объеме. Контроль и совершенствование реализации мер ЗИ происходит эпизодически
Четвертый	От 0,85 до 0,9 (включительно)	Меры осуществляются в полном объеме. Контроль и совершенствование реализации мер ЗИ в основном обеспечены
Пятый	От 0,9 до 1	Меры осуществляются в полном объеме. Контроль и совершенствование реализации меры ЗИ обеспечены в полном объеме

КОД БЕЗОПАСНОСТИ

Сроки действия уровней соответствия для КФО

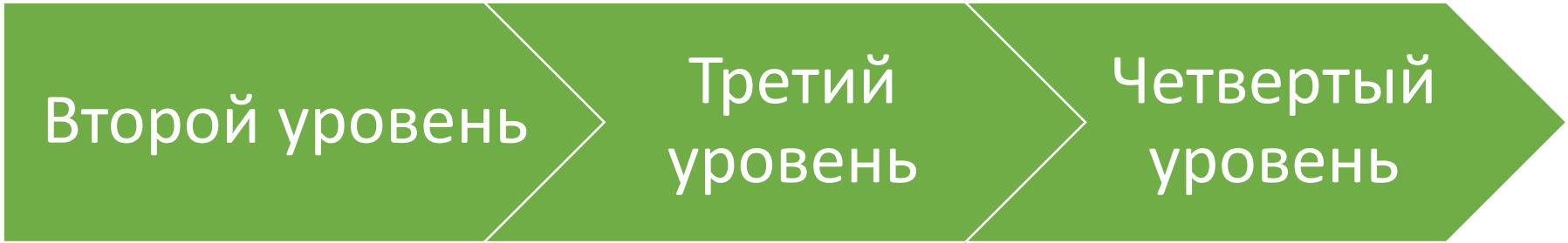
01.01.2021 **01.01.2022**



КОД БЕЗОПАСНОСТИ

Сроки действия уровней соответствия для НФО

01.01.2022 **30.06.2023**



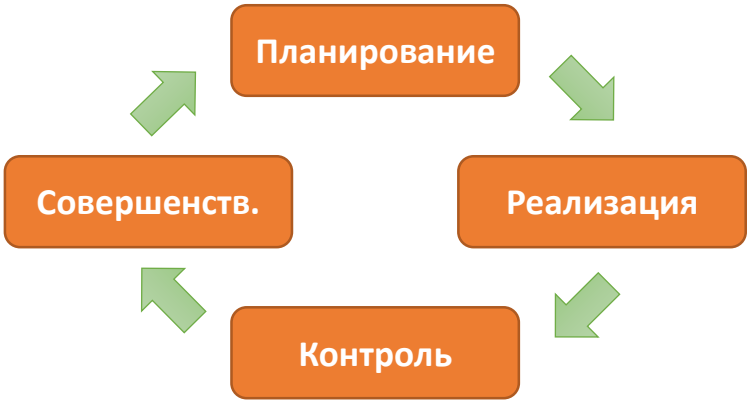
КОД БЕЗОПАСНОСТИ

Как получить значение соответствия? Сначала о терминах

Процессы системы защиты информации:

- Защита информации при управлении доступом
- Защита вычислительных сетей
- Контроль целостности и защищенности
- Защита от вредоносного кода
- Предотвращение утечек информации
- Управление инцидентами
- Защита среды виртуализации
- Защита удаленного доступа

Организация и управление защитой информации:



Защита информации на этапах жизненного цикла:

Меры защиты на этапах создания, модернизации, ввода в эксплуатацию, сопровождения, вывода из эксплуатации

Выводы

- Все процессы системы защиты информации равны
- Чем меньше мер в процессе, тем выше ее влияние на общий показатель процесса
- Меры управления защитой информации оказывают сильное влияние на оценку и при этом:
  - Содержат мало мер
  - Разрешают частичное выполнение меры
- Грубые нарушения очень сильно влияют на оценку, их надо устранить в первую очередь ☺

Про технологии обработки защищаемой информации

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

Про требования к обработке к информации

Поиск уязвимостей

КОД БЕЗОПАСНОСТИ

Два разных ОУДа

- П.4.1 предписывает использование клиентского и серверного ПО для дистанционного банковского обслуживания которое:
  - Либо **сертифицировано ФСТЭК** по каким-либо требованиям безопасности включая требования по анализу уязвимостей и отсутствию НДВ
  - Либо в отношении которого был проведен анализ уязвимостей по требованиям ОУД 4 в соответствии со **ГОСТ 15408-3-2013 и профилем защиты**

Про проверки

КОД БЕЗОПАСНОСТИ

Требования к аудиту

- Внешний аудит нужен для:
  - Анализ уязвимостей в ПО
  - Соответствие ГОСТ 57580.1
- Проводится раз в два года
- Требования к аудитору – лицензия ФСТЭК на ТЗКИ, предусматривающая проведение:
  - Работ по контролю защищенности конфиденциальной информации (пп «Б»)
  - Работ по проектированию средств и систем информатизации в защищенном помещении (пп «Д»)
  - Работ по установке средств защиты, обработки и контроля эффективности защиты информации (пп «Е»)

КОД БЕЗОПАСНОСТИ

Action plan

Проаудировать ИТ-инфраструктуру на соответствие ГОСТ 57580

Организовать процесс поиска уязвимостей в платежном ПО собственной разработки по ГОСТ 15408 и профилю защиты ЦБ

Установить требования для поставщиков платежного ПО по поиску уязвимостей в соответствии с ГОСТ 15408 и профилем защиты

Оценить необходимость доработки систем ФО в соответствии с требованиями к обработке защищаемой информации

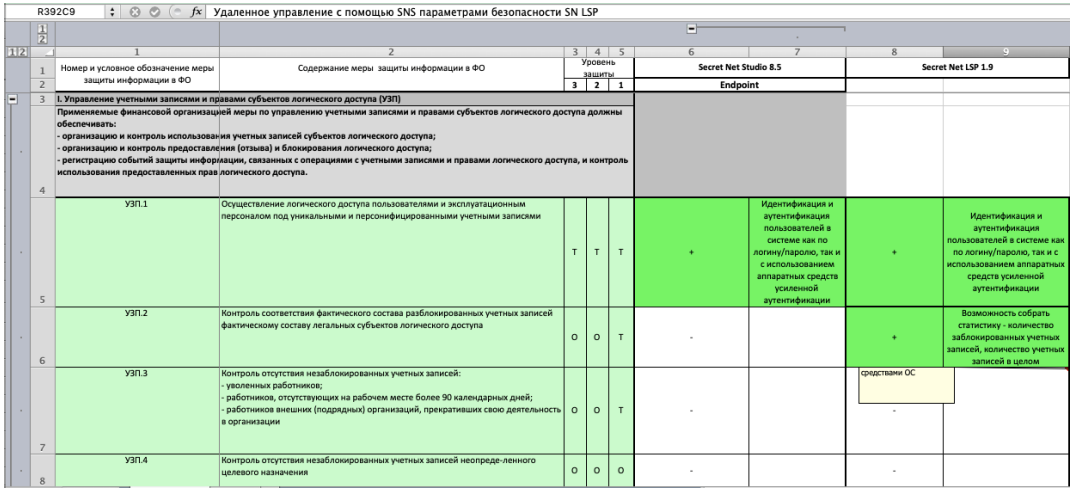
Организовать процесс реагирования на инциденты ИБ и информирования регуляторов

Стартовать процесс перехода на безбумажный документооборот

КОД БЕЗОПАСНОСТИ

Специально для вас!

- Собрали все меры ГОСТ 57580.1 в единый файл
- Оценили выполнение нашими продуктами этих мер
  - Secret Net Studio + Secret Net LSP
  - Континент
  - vGate
  - Соболь



R392C9 | Удаленное управление с помощью SNS параметрами безопасности SN LSP

Номер и условное обозначение меры защиты информации в ФО	Содержание меры защиты информации в ФО	Уровень защиты 3	4	5	Secret Net Studio 8.5 Endpoint		Secret Net LSP 1.9	
I. Управление учетными записями и правами субъектов логического доступа (УЗП)								
Применяемые финансовой организацией меры по управлению учетными записями и правами субъектов логического доступа должны обеспечивать: - организацию и контроль использования учетных записей субъектов логического доступа; - организацию и контроль предоставления (отзыва) и блокирования логического доступа; - регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.								
УЗП.1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	Т	Т	Т	+	Идентификация и аутентификация пользователей в системе как по логину/паролю, так и с использованием аппаратных средств усиленной аутентификации	+	Идентификация и аутентификация пользователей в системе как по логину/паролю, так и с использованием аппаратных средств усиленной аутентификации
УЗП.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	О	О	Т	-		+	Возможность собрать статистику - количество заблокированных учетных записей, количество учетных записей в целом
УЗП.3	Контроль отсутствия незаблокированных учетных записей: - уволенных работников; - работников, отсутствующих на рабочем месте более 90 календарных дней; - работников внешних (подрядных) организаций, прекративших свою деятельность в организации	О	О	Т	-		средствами ОС -	
УЗП.4	Контроль отсутствия незаблокированных учетных записей неопреде-ленного целевого назначения	О	О	О	-		-	

Спасибо за внимание!

КОД БЕЗОПАСНОСТИ

Павел Коростелев
p.korostelev@securitycode.ru
Подходите на стенд B75

info@securitycode.ru
http://securitycode.ru