

# *О вопросах совершенствования информационной безопасности организаций кредитно-финансовой сферы*



**Банк России**

**О.В. Крылов**

Начальник Главного управления  
безопасности и защиты информации  
Банка России

# Влияние информационной безопасности на деятельность кредитных организаций.

- Риски информационной безопасности в значительной степени интегрированы с основными банковскими рисками, среди которых в первую очередь выделяются операционные, правовые и репутационные риски.
- Процессы обеспечения информационной безопасности в Банке России и кредитных организациях зависят от ряда внешних факторов, основные из которых:
  - изменения в законодательстве Российской Федерации;
  - изменения в информационных технологиях, применяемых в Банке России и кредитных организациях.



# Комплекс документов в области стандартизации «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»

- Совершенствование указанного комплекса необходимо для использования Банком России и кредитными организациями актуальной методологической базы, адаптированной под цели и задачи деятельности Банка России и кредитных организаций.
- Требуется доработка, основной целью которой будет отображение и учет практики и специфики деятельности Банка России и кредитных организаций в составе требований и рекомендаций Комплекса.
- Использование документов Комплекса показывает определенный уровень зрелости кредитной организации в вопросах обеспечения информационной безопасности и повышает доверие к ее деятельности.

# Основные факторы, способствующие повышению эффективности обеспечения информационной безопасности:

- оптимизация и автоматизация деятельности подразделений защиты информации на этапе создания и ввода в эксплуатацию автоматизированных банковских систем;
- внедрение автоматизированных технологий контроля и мониторинга обеспечения информационной безопасности на этапе эксплуатации автоматизированных банковских систем;
- оптимизация и автоматизация организационных процедур деятельности подразделений защиты информации по контролю состояния обеспечения информационной безопасности.



# Основные направления деятельности подразделений защиты информации на этапе создания и ввода в эксплуатацию автоматизированных банковских систем

- Поэтапный переход от концепции обеспечения защиты информации в автоматизированных банковских системах, реализуемой путем создания подсистем информационной, к реализации концепции создания защищенной среды, реализуемой комплексным и согласованным применением систем и средств защиты информации и организации процессов управления ими, преимущественно по инфраструктурному (объектовому) принципу.
- Переориентация на сопровождение работ по созданию типовых комплексных решений для реализации концепции защищенной среды информационно-телекоммуникационной системы структурных подразделений кредитных организаций.
- Унификация и типизация применяемых систем и средств защиты информации, внедряемых в структурных подразделениях кредитных организаций.



## Основные направления деятельности подразделений защиты информации на этапе эксплуатации автоматизированных систем в части внедрения автоматизированных технологий контроля и мониторинга обеспечения информационной безопасности

- Внедрение автоматизированного мониторинга действий администраторов и пользователей автоматизированных банковских систем и выявление нарушений регламентов эксплуатации автоматизированных банковских систем;
- Автоматизация контроля эксплуатации применяемых средств и систем защиты информации, в том числе контроль настроек указанных средств и систем;
- Автоматизация контроля использования электронной почты и ресурсов сети Интернет, а также контроля, направленного на предотвращение утечек конфиденциальной информации.

# Совершенствование деятельности подразделений защиты информации по выполнению процедур контроля обеспечения информационной безопасности

Делегирование контрольных функций специально назначенным работникам- администраторам информационной безопасности



Осуществление администраторами информационной безопасности полного контроля обеспечения информационной безопасности, входящий в их зону ответственности, с установленной периодичностью и использованием методических документов, разработанных подразделениями защиты информации



Деятельность подразделений защиты информации фокусируется на контроле деятельности администраторов информационной безопасности, при этом осуществляется выборочная перепроверка их деятельности



**Спасибо за внимание!**



**Крылов Олег Вячеславович**  
Начальник Главного управления безопасности  
и защиты информации Банка России