Современные информационные технологии и кибербезопасность

А.М. Шойтов
Заместитель министра Минцифры России
Президент Академии криптографии
Российской Федерации

2022

Особо значимые достижения в реализации федерального проекта за 2021 год ✓

2 сегмента **киберполигона** «ИТ-киберполигон» и «Индустриальный киберполигон» введены в промышленную эксплуатацию и в опытную эксплуатацию сегмент для нефтегазового комплекса.

Введен в эксплуатацию отраслевой центр Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (**ГосСОПКА**) (1 очередь).

Введен в промышленную эксплуатацию **национальный удостоверяющий центр**, предназначенный для выпуска сертификатов безопасности (TLS/SSL - сертификаты).

Введена в опытную эксплуатацию информационная система, предназначенная для мониторинга **фишинговых сайтов.**

Запущен проект по аудиту защищенности ГИС на уязвимости. Осуществлен независимый анализ защищенности

9 ГИС Минцифры России

В рамках достижения результата «Создан и функционирует национальный технологический центр внедрения методов современной криптографии» **выполнены**

1 опытно-конструкторская работа по разработке линейки средств защиты информационного взаимодействия сетей связи общего пользования,

2 научно-исследовательские работы (НИР)

и **первые этапы 3 НИР** в сфере перспективного применения криптографической защиты информации.

В рамках реализации мероприятий, направленных на подготовку кадров в области информационной безопасности:

- более **4 тысяч специалистов** прошли практико-ориентированное обучение в области кибербезопасности
- предоставлены **30 грантов** на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики
- осуществлены повышение квалификации и профессиональная переподготовка профессорско-преподавательского состава в области информационной безопасности в количестве **402 слушателей**
- проведен ряд интеллектуальных соревнований среди молодежи, ориентированной на деятельность в области информационной безопасности

Направления научно-исследовательских работ, выполняемых в Академии криптографии Российской Федерации в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»

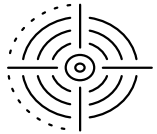
Выполнены 16 НИР по направлениям:

- Исследование криптографических механизмов и протоколов, применяемых в системах беспроводной связи - 4 НИР;
- исследование криптографических методов защиты информации квантовых вычислительных систем - 1 НИР;
- исследование криптографических алгоритмов защиты информации платежных систем - 2 НИР;
- исследование криптографических алгоритмов защиты информации платежных систем – 2 НИР;
- исследование проблем информационной безопасности облачных вычислений – 1 НИР;
- исследование проблем выявления инцидентов информационной безопасности – 1 НИР;
- исследование проблем информационной безопасности систем распределенных реестров – 2 НИР;
- и другие.

Проводятся 10 НИР по направлениям:

- Исследование криптографических механизмов идентификации и аутентификации – 2 НИР;
- исследование базовых криптографических алгоритмов – 1 НИР;
- исследование криптографических алгоритмов защиты информации платежных систем – 1 НИР;
- исследование криптографических механизмов и протоколов, применяемых в системах беспроводной связи – 1 НИР;
- исследование проблем выявления инцидентов информационной безопасности – 1 НИР;
- исследование проблем информационной безопасности при использовании облачных вычислений – 2 НИР;
- и другие.

Планируется поставить 6 НИР по следующим направлениям:



- Исследование криптографических механизмов и протоколов, применяемых в системах, использующих технологии искусственного интеллекта - 1 НИР;
- исследование базовых криптографических алгоритмов - 1 НИР;
- исследование криптографических алгоритмов защиты информации платежных систем - 2 НИР;
- исследование проблем выявления инцидентов информационной безопасности - 2 НИР.

Деятельность Академии криптографии Российской Федерации в рамках федерального проекта «Искусственный интеллект»

Цель:

Формирование научной базы для современных защищенных технологий и систем ИИ, применяемых в государственных информационных системах

Задачи:

Проведение научных исследований в области обеспечения информационной безопасности при применении ИИ, разработка требований по обеспечению информационной безопасности в системах, реализующих ИИ

Сроки:

2021 – 2024

2020 – 2021

Общие вопросы СИИ. Анализ угроз, методов защиты, концепция построения требований к СИИ.

2021 – 2022

- Применение ИИ для защиты от компьютерных атак;
- эффективность методов обезличивания, анализ угроз деобезличивания;
- методы защиты СИИ криптографическими методами: гомоморфное шифрование, протоколы безопасных многосторонних вычислений;
- построение обучающих выборок. Разработка модели нарушителя на этапе обучения СИИ и методов защиты;
- определение авторства с помощью ИИ.

2022 – 2023

- Интерпретация результатов работы СИИ;
- эффективность методов обезличивания, анализ угроз деобезличивания;
- методы защиты СИИ криптографическими методами: гомоморфное шифрование, протоколы безопасных многосторонних вычислений;
- безопасность ИИ в автономных транспортных средствах;
- безопасность биометрических систем идентификации с ИИ.

Информационная безопасность и развитие квантовых технологий в Национальной программе «Цифровая экономика Российской Федерации»

НИОКР серии «Утро»

Завершены НИОКР серии «Утро» по созданию уникальных комплексов технических средств и методического обеспечения для оснащения одной экспертной, двух испытательных лабораторий и одного учебно-испытательного центра в целях обеспечения внедрения квантовых криптографических систем в национальные волоконно-оптические сети связи. Осуществляются мероприятия по организационному и юридическому их оформлению как элементов в цепочке сертификационных исследований, направленных на реализацию и внедрению отечественных систем КРК с высокими характеристиками информационной безопасности.

Осуществляется цикл научно-исследовательских работ в Академии криптографии Российской Федерации по оценке криптографических свойств существующих, обоснованию параметров и разработке новых алгоритмов, протоколов, и механизмов для постквантовой криптографии, обеспечивающих точное понимание и выработку необходимых мероприятий для своевременного реагирования на вызовы «квантовой революции», в том числе и в части стандартизации в области криптографии.

Новый подход к обеспечению ИБ в облачных платформах

	ФОИВ (владелец ГИС)	Операторы ГИС и компонентов	Внешние (независимые) организации
	Обеспечение функционирования бизнес-процесса	Обеспечение работоспособности и защищенности	Выявление кибератак и управление реагированием
Создание ГИС	**Определение класса защиты:** ▪ Определение автоматизируемых бизнес-процессов и ФТ к ГИС ▪ Определение видов и объемов защищаемой информации ▪ Моделирование угроз и определение классов защиты	**Реализация мер защиты:** ▪ Адаптация типовых решений ▪ Внедрение и настройка СЗИ (облачных и on-prem) ▪ Проведение аттестации и перевода системы в эксплуатацию	**Согласование методов защиты:** ▪ Определение требований к методам обеспечения ИБ ▪ Формирование типовых решений по обеспечению ИБ ▪ Определение требований к процессам ИБ
Эксплуатация и обеспечение ИБ	**Функционирование бизнес-процесса:** ▪ Контроль функционирования ГИС и эффективности исполнения бизнес-процессов ▪ Разработка и отработка планов аварийного функционирования	**Реагирование и восстановление:** ▪ Обеспечение работоспособности ГИС ▪ Эксплуатация средств защиты ▪ Реагирование на инциденты ИБ ▪ Восстановление работоспособности	**Выявление атак и управление отражением:** ▪ Мониторинг и контроль защищенности ▪ Управление реагированием на кибератаки ▪ Разработка тех. политик ▪ Аналитика и корректировка мер

Спасибо за внимание