Современная информационная безопасность (ИБ) криптографических средств(КрС)

Надежность защиты информации теперь определяется не только криптосхемой и ее ключевой структурой , но и комплексно аппаратным окружением вместе с информационным пространством, в условиях непрерывных попыток технического воздействия и дезинформации. Отрицанием положительного с навязыванием ложного

Понимание надежности криптосредств

- Массовые пользователи уповают на аттестацию компетентных органов и выполнение их требований разработчиками решений. При этом правила применения, требуемые регулятором, пользователем редко соблюдаются
- Компетентные специалисты в области математического анализа криптопреобразований считают, что если неизвестны методы определения ключа с определенной трудоемкостью, то все надежно защищено
- Отсутствие известных методов может быть математически доказано, а может и являться следствием чрезвычайной сложности самого криптопреобразования. Последнее относится к наиболее применяемым блочным, многоитеративным шифрам и видам электронной подписи
- Специалисты по применению КрС знают, что окружающая компьютерная среда определяет надежность защиты информации не меньше чем сама криптосхема или схема выработки действующего ключа
- Все три компоненты ИБ криптосредств- конфиденциальность(К), целостность(Ц) и доступность(Д) полностью относятся к обеспечению целевого применения криптографии в компьютерных системах

ИБ исследований КрС

- ИБ непосредственно связано с информационным нападением-введением в заблуждение или дезинформацией. Для направления исследований по ложному пути применяются все доступные способы одурачивания противника и маркетинговые приемы. Попутно распыляются финансовые ресурсы лишая по настоящему полезные направления материальной основы
- Исследования криптосхем ориентируются на некоторый гипотетический вычислитель(ГВ). Результат это прогноз на основе математической фантазии автора. Популярный ГВ это сейчас универсальный кубитный компьютер произвольной фантазийной архитектуры, а в прошлом веке параллелилизм был фантазией. ИБ принятия решений о стойкости криптосхемы включает в том числе и защиту от дезинформации в области реальности прогноза
- Универсальная архитектура квантового комьпьютера это утопия, за 50 лет идеи, реализованная для 10 произвольно связываемых под задачу кубитов
- В реальных задачах требуются сотни и тысячи связываемых определенным для конкретной задачи образом кубитов, перестраиваемых в рамках выбранной архитектуры под другую задачу
- Имеющиеся в мире комплексы на 100 и более кубитов реализуют некоторые фиксированные схемы квантового спутывания, определяющие одну или узкий класс задач, не имеющих практического применения

Квантовые исследований КрС

- Современная вычислительная техника начиналась с построения технического комплекса для определения ключа шифратора Энигма и применения аналоговых схем для решения дифференциальных уравнений
- С 2020 года известно и стало быстро технически развиваться направление фотонных, квантовых симуляторов(ФКС), состоящих из излучателей, светоделителей и счетчиков одиночных фотонов
- Суть этого направления заключается в реализации, как и в квантовых, кубитных компьютерах, случайного, физического процесса на основе случайности отражения-пропускания одиночных фотонов светоделителями
- ФКС может быть использован для получения оценки перманента матрицы, вычисление которого относится к NP-полной задаче и в частности, как удалось установить, решению системы булевых уравнений в 3-ДНФ
- Ряд задач в конечных полях также можно свести к решению систем булевых уравнений в 3-ДНФ форме. Построение компактных систем 3- ДНФ соответствующих исходной задаче, как правило требует определенного искусства и фантазии исследователя в области логического криптоанализа

Развитие Требований КС1- КА

- Сформированный еще в 2010 году подход к формированию классов КС1-КА исходит из описания возможностей нападающей стороны на результат применения КС по дешифрованию информации или подделке ЭП
- Чем большими возможностями обладает предполагаемый противник, тем выше должен быть класс защиты. Подразумевается, что чем ценней информация, тем больший ресурс может привлечь нападение. В конкретных системах и условиях это не всегда верно и определить какому противнику будет нужна защищаемая информация сложно без оперативных данных
- Реально класс средств выбирается из возможностей обеспечения требований в компьютерной системе, реализующей необходимый набор прикладных функций, допускающих некоторую защиту
- Главное- обеспечить функционал системы, а затем защиту информации. Поэтому определенная формализация последствий для информации в компьютерной системе для различных классов требований востребована
- Последствия связаны со средой применения , выполнением обязанностей пользователем и обслуживающим персоналом, используемых видов ППО

Наблюдаемые сейчас методы проникновения и классы защиты собственно криптосистем

- Нападающая сторона- хулиганы, террористы, вымогатели или спецслужбы. Примеры уровней защиты:
- Хулиганы- КС1, КС2. Массовый сегмент только ЦС1.Требуется двухфакторная идентификация
- Террористы- два подхода: внутренний, малокомпетентный, запуганный пользователь или внешний компетентный хакер-специалист- КС3, КБ. В системах более 100 пользователей КБ реализовать тяжело, но возможно
- Вымогатель- КС3- КА. Выход на внутреннего нарушителя как осознанного, так и жертву фишинга. При наличии подключения к Интернет всегда есть риск наличия внутреннего противника, который может и не знать, что его пароль используется для проникновения
- Отчуждаемый, необлачный носитель – гарантия восстановления за приемлемое время системы после нападения, даже с атакой разрушения
- Сегментирование и изоляция от Интернета ответственного сегмента обязательная мера защиты, как бы это не было неудобно пользователям

Содержание понятия ИБ для КрС

- К, Ц, Д : для ключа и ключевой схемы, для криптосхемы, для хеш функции при выработке ЭП
- ИБ средств, взаимодействующих с КрС: какая информация обрабатывается КрС, из какого ресурса поступает, для какого получателя, с чем и как взаимодействует система даже без применения КрС
- ИБ шифрования и выработки ЭП для «чуствительной» , например персональные данные, информации при ее хранении в системе, включая отчуждаемые носители основывается на анализе и контроле актуального, адекватного описания самой системы, что почти повсеместно отсутствует
- ИБ для КрС канала «асимметричного» шифрования посредством технологии открытого ключа требует подтверждения сертификата партнера, в независимой от провайдера шифруслуги системе, для исключения реализации «встречи посередине»
- При проверке правильности ЭП обеспечение ИБ системы включает подтверждение сертификата через запрос соответствующего УЦ, что часто не делается. По QR-коду смартфоном вычисляется ЭП, при отсутствии связи с УЦ

Выводы и предложения

- Как и ранее надежность КрС определяется отсутствием эффективного способа определения ключа в классе известных методов анализа, в том числе и за счет невозможности современного понимания сложности многоитеративного преобразования и его альтернативного представления
- Прогноз изменения оценки надежности должен базироваться на реальных направлениях развития электронно-технических устройств в предыдущие 20-30 летия, основываясь на достигнутых, а не фантазийных результатах
- Квантовые алгоритмы решения математических и криптографических задач, основанные на эксплуатации стохастических процессов, находятся в состоянии технической реализации отдельных фиксированных задач. Надо понять и выделить тип технического устройства, которое поможет эффективно решать достаточно большой класс NP-полных задач
- Требования КС1-КА предлагается дополнить перечнем последствий для информационной системы применения
- ИБ для КрС в компьютерных системах является следствием общего уровня безопасности информации, включая пользователей, обслуживающий персонал, архитектуру и оценку ИБ импортозамещеных компонент