МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

Направление подготовки	**08.03.01**
Направленность (профиль)	Строительство
Квалификация выпускника	Бакалавр

РАЗРАБОТАНО:
Доцент кафедры СУиИТ
_____ Мишин В.В.
«____» _____ 2020 г.

Пятигорск, 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Методические рекомендации содержат перечень тем с вопросами для самостоятельной проработки, перечень практических работ с вопросами для самостоятельной проработки.

Методические указания посвящены курсу «Персональная кибербезопасность». Кибербезопасность являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Кибербезопасность является необходимым условием развития информационного общества.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Персональная кибербезопасность» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки **08.03.01**

Задачи освоения дисциплины: изучение основных понятий кибербезопасности, освоение навыков соблюдения персональной кибербезопасности.

2. ТЕМЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов*
	2 семестр	

	Раздел 1. Концепции персональной кибербезопасности	
1	Тема 1. Основные понятия персональной кибербезопасности	7
	Раздел 2. Технологии организации персональной кибербезопасности	
5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности	8
	Итого за 2 семестр	15

3. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩЕГОСЯ

4. РЕКОМЕНДАЦИИ ДЛЯ САМОПОДГОТОВКИ

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-2	Подготовка к лекциям	Конспект	Собеседование	11,88	0,12	12
ОПК-2	Самостоятельное изучение литературы по темам 1, 5	Конспект	Собеседование	2,97	0,03	3
			Итого	13, 5	1,5	15

4.1 Подготовка к лекциям. Самостоятельное изучение литературы

Базовый уровень

Тема 1. Основные понятия персональной кибербезопасности

1. Информационная безопасность и кибербезопасность.
2. Свойства оцифрованной информации.
3. Причины киберпреступлений.
4. Проблемы кибербезопасности.
5. Анализ рисков как основа управления персональной кибербезопасностью
6. Модель угроз STRIDE.
7. Инструменты анализа и контроля информационных рисков.
8. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, STRIDE

Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности

9. Оценка средств криптозащиты.
10. Экономическое обоснование расходов на обеспечение персональной кибербезопасности.
11. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности.
12. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

Повышенный уровень

Тема 1. Основные понятия персональной кибербезопасности

13. Основные понятия кибербезопасности.
14. Характеристики оцифрованной информации.
15. Классификация киберпреступлений.
16. Технологии кибербезопасности.
17. Управление персональной кибербезопасностью
18. Характеристики модели угроз STRIDE.
19. Инструменты анализа и контроля информационных рисков.
20. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: Гексада Паркера, 5A, STRIDE

Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности

21. Набор финансово-экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций.
22. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности.

4.2 Подготовка к практическим работам

Базовый уровень

Тема 1. Основные понятия персональной кибербезопасности

1. Информационная безопасность и кибербезопасность.
2. Свойства оцифрованной информации.
3. Причины киберпреступлений.
4. Проблемы кибербезопасности.

Тема 2. Моделирование угроз персональной кибербезопасности

5. Анализ рисков как основа управления персональной кибербезопасностью
6. Модель угроз STRIDE.
7. Инструменты анализа и контроля информационных рисков.
8. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, STRIDE

Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности

9. Оценка средств криптозащиты.
10. Экономическое обоснование расходов на обеспечение персональной кибербезопасности.
11. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности.
12. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

Тема 6. Инструменты организации персональной кибербезопасности

13. Обзор антивирусных средств защиты при организации системы персональной кибербезопасности.
14. Антивирусная защита персональных компьютеров и мобильных устройств.
15. Брандмауэры.
16. Компоненты аппаратных средств защиты информации.

Тема 7. Персональная кибербезопасность в интернет-банкинге

17. Интернет-банкинг.
18. Технологии защиты в интернет-банкинге.
19. Причины киберпреступлений в интернет-банкинге.
20. Проблемы кибербезопасности в интернет-банкинге.

Повышенный уровень

Тема 1. Основные понятия персональной кибербезопасности

1. Основные понятия кибербезопасности.

2. Характеристики оцифрованной информации.
3. Классификация киберпреступлений.
4. Технологии кибербезопасности.

Тема 2. Моделирование угроз персональной кибербезопасности

5. Управление персональной кибербезопасностью
6. Характеристики модели угроз STRIDE.
7. Инструменты анализа и контроля информационных рисков.
8. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: Гексада Паркера, 5A, STRIDE

Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности

9. Набор финансово-экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций.
10. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности.

Тема 6. Инструменты организации персональной кибербезопасности

11. Средства аппаратной защиты информации.
12. Организация программно-аппаратных средств персональной кибербезопасности.

Тема 7. Персональная кибербезопасность в интернет-банкинге

13. Интернет-банкинг.
14. Технологии защиты в интернет-банкинге.
15. Причины киберпреступлений в интернет-банкинге.
16. Проблемы кибербезопасности в интернет-банкинге.

5. ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

5.1 ОСНОВНЫЕ ПОНЯТИЯ ПЕРСОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Основные понятия персональной кибербезопасности

Во времена Римской империи была сформулирована геополитическая формула: "Кто владеет морем, тот владеет миром!" Во время Второй мировой войны это выражение было модифицировано и звучало уже следующим образом: "Кто владеет воздушным пространством, тот владеет миром!" И наконец, во второй половине XX века, в период становления постиндустриального общества был выработан новый геополитический тезис: "Кто владеет информацией, тот владеет миром!", который остается актуальным и по сей день.

Наступило время, когда необходимо считаться с тем, что переход информации в разряд важнейших ресурсов человечества одновременно порождает проблему обладания этим ресурсом, его уничтожения или изменения, исходя из государственных, коммерческих, частных и других интересов, и, как следствие, приводит к появлению нового средства нападения или защиты, т.е. информационного оружия. Причиной такой перемены стала возможность представления информации в цифровом виде. Важно отметить, что цифровая информация обладает следующими неотъемлемыми свойствами

Отчуждаемость

Воспроизводимость

Неуничтожимость

Возможность быстрого поиска

С одной стороны, эти качества позволяют существенно оптимизировать процесс обработки информации, сведя к минимуму вмешательство человека в рутинные процессы и обеспечивая легкий и быстрый доступ к необходимым сведениям. С другой стороны, они же стали причиной появления в конце XX в. нового вида злодеяний -

киберпреступлений. Так, отчуждаемость и воспроизводимость информации вкупе привели к обострению проблемы защиты авторских прав. Не так давно понятие "кража" подразумевало, что субъект лишается неких материальных ценностей. С цифровой информацией все по-другому: если пират копирует диск с записью еще не вышедшего фильма, имущество правообладателя может физически не пострадать - однако при этом законный хозяин теряет над своим произведением контроль. Более того, если до появления компьютеров создание дубликатов приводило к ухудшению качества объекта копирования (репродукции картин, переписывание книг и аудиокассет и т.д.), то в цифровом мире копирование может производиться в неограниченных количествах практически бесплатно - и без потери качества! К парадоксально нежелательным результатам привело и быстрое снижение цен на устройства хранения данных. Работа по анализу хранимой в организации информации с целью выявления данных, подлежащих уничтожению по причине утери актуальности и полезности, обходится дороже покупки и установки нового оборудования. Вследствие этого новостные ленты пестрят заголовками о найденных в мусоре или купленных на аукционах жестких дисках и магнитных лентах, содержащих секретные сведения, которые никто не потрудился стереть перед утилизацией устройств. Отдельного внимания заслуживает проблема уничтожения информации, хотя бы однажды появившейся в Интернет и проиндексированной поисковой системой. Возможность быстрого поиска и объединения по ключевым полям (например, ФИО и адрес электронной почты) делает задачу составления портрета активного пользователя компьютера максимально простой для злоумышленника.

Как следствие этого острота проблемы обеспечения информационной безопасности (ИБ) субъектов информационных отношений, защиты их законных интересов при использовании информационных систем и сетей, хранимой, обрабатываемой и передаваемой в них информации постоянно возрастает. Несмотря на интенсивное внедрение вновь создаваемых технологических решений в области информационной безопасности, уровень криминогенности в информационной сфере сетей передачи данных ведущих стран мира постоянно повышается, что приводит к миллиардным финансовым потерям.

По данным координационного центра немедленного реагирования CERT, организованного при университете Карнеги Меллона, ежегодно наблюдается рост количества регистрируемых информационных атак (рис. 1.1). Как видно на диаграмме, одной из наиболее актуальных проблем в последнее время стала защита от инсайдеров (сотрудников компании, являющийся нарушителем, который может иметь легальный доступ к конфиденциальной информации). Такая угроза стала возможной во многом из-за появления портативных и дешевых устройств хранения с высокой плотностью записи. Обостряет ситуацию мировой финансовый кризис, в условиях которого выросло число сотрудников, недовольных своим работодателем (вследствие сокращения зарплаты или даже увольнения) и желающих нанести ему вред или незаконно обогатиться.

Рис. 1.1. Рост количества атак

Характерно, что количество компьютерных преступлений, совершаемых в России, ежегодно увеличивается. Так, согласно статистике Министерства внутренних дел РФ, количество компьютерных преступлений, связанных с несанкционированным доступом к конфиденциальной информации, увеличилось с шестисот инцидентов в 2000 г. до семи тысяч в 2004 г. К основным причинам роста количества атак можно отнести следующие факторы:

с каждым годом увеличивается количество пользователей общедоступных сетей связи, таких, например, как сеть Интернет. При этом в качестве новых пользователей выступают как отдельные клиентские рабочие станции, так и целые корпоративные сети;

увеличивается количество уязвимостей, ежедневно обнаруживаемых в существующем общесистемном и прикладном программном обеспечении;

возрастает число возможных объектов атаки. Если несколько лет назад в качестве основных объектов несанкционированного воздействия рассматривались исключительно серверы стандартных Web -служб, такие как HTTP, SMTP и FTP, то к настоящему моменту разработаны средства реализации атак на маршрутизаторы, коммутаторы, межсетевые экраны и др.;

упрощаются методы реализации информационных атак. В сети Интернет можно без труда найти программные реализации атак, направленных на активизацию различных уязвимостей. При этом использование этих средств сводится к вводу IP -адреса объекта атаки и нажатию соответствующей управляющей кнопки;

увеличивается число внутренних атак со стороны пользователей автоматизированных систем (АС). Примерами таких атак является кража конфиденциальной информации или запуск вредоносного программного обеспечения (ПО) на рабочих станциях пользователей.

Необходимо отметить, что уровень сложности информационных атак также постоянно растет. Данное утверждение можно проиллюстрировать на примере эволюции компьютерных вирусов. В момент своего первого появления в 1980 г. вирусы представляли собой достаточно простые программы, которые самостоятельно распространялись в автоматизированных системах и основной задачей которых было нарушение работоспособности системы. Сегодня же компьютерные вирусы представляют существенно более сложные программные средства, способные распространятся практически в любой среде передачи информации, а также маскироваться под работу штатного ПО. Кроме этого, современные модификации компьютерных вирусов в основном используются для кражи конфиденциальной информации, а также для получения несанкционированного доступа к компьютерам пользователей. Аналогичная тенденция характерна и для других видов угроз безопасности, для реализации которых постоянно придумываются более изощренные методы и средства проведения атак.

Изменилась и ментальность хакеров: если раньше основной мотивацией было решение сложной проблемы и возможность самоутверждения, то сегодня на первый план выходит коммерческая составляющая, которая способствует объединению талантливых одиночек в организованные преступные сообщества.

Стоит обратить внимание на положительную тенденцию - некоторые производители программного и аппаратного обеспечения стали обращать внимание на безопасность продукта уже на стадии проектирования, а не в последний момент, когда изменить что-либо в архитектуре системы уже поздно и можно довольствоваться функциональными "заплатками". Однако и на этом пути есть препятствия: во-первых, производство продукта, не содержащего ошибок, в реальном мире невозможно; во-вторых, компьютер представляет собой систему из огромного числа компонентов от разных вендоров, и тестирование совместной работы всевозможных комбинацией является неразрешимой задачей. Наконец, самая совершенная защита может быть взломана, и причина этому - человеческий фактор. Устранить эту угрозу принципиально невозможно, т.к. персонал является неотъемлемой частью любой информационной системы.

С учетом вышесказанного можно с уверенностью утверждать, что проблема защиты АС от информационных атак является одной из наиболее актуальных и значимых в ИТ-индустрии. По всему миру ежегодно проводится большое количество исследований, направленных на разработку новых и более эффективных методов противодействия угрозам злоумышленников. С учетом актуальности вопросов, связанных с защитой от внешних и внутренних информационных атак, и был написан этот учебный курс.

Краткие итоги

В данной лекции были рассмотрены фундаментальные свойства оцифрованной информации и их влияние на рост угроз в сфере информационной безопасности с наступлением компьютерной эры. Перечислены факторы, не позволяющие обеспечить совершенную защиту информации, и выделен перечень не решенных на данный момент проблем.

5.2. МОДЕЛИРОВАНИЕ УГРОЗ ПЕРСОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Моделирование угроз персональной кибербезопасности

Основой управления информационной безопасностью предприятия является анализ рисков. Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам.

Обычно выделяют две основные группы методов расчёта рисков безопасности. Первая группа позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. В качестве источников таких требований могут выступать (рис. 3.1):

Нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности;

Требования действующего российского законодательства - руководящие документы ФСТЭК (Гостехкомиссии), СТР-К, требования ФСБ РФ, ГОСТы и др.;

Рекомендации международных стандартов - ISO 17799, OCTAVE, CoBIT и др.;

Рекомендации компаний-производителей программного и аппаратного обеспечения - Microsoft, Oracle, Cisco и др.

Рис. 2.1. Источники требований информационной безопасности, на основе которых может проводиться оценка рисков

Вторая группа методов оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита.

Методы первой и второй группы могут использовать количественные или качественные шкалы для определения величины риска информационной безопасности. В первом случае риск и все его параметры выражаются в числовых значениях. Так, например, при использовании количественных шкал вероятность проведения атаки может выражаться числом в интервале , а ущерб атаки может задаваться в виде денежного эквивалента материальных потерь, которые может понести организация в случае успешного проведения атаки. При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определённый интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от применяемых методик оценки рисков. В таблицах 3.1 и 3.2 приведены примеры качественных шкал оценки рисков информационной безопасности, в которых для оценки уровней ущерба и вероятности атаки используется пять понятийных уровней.

Таблица 3.1. Качественная шкала оценки уровня ущерба

№	Уровень ущерба	Описание
1	Малый ущерб	Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании
2	Умеренный ущерб	Вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании
3	Ущерб средней тяжести	Приводит к существенным потерям материальных активов или значительному урону репутации компании
4	Большой ущерб	Вызывает большие потери материальных активов и наносит большой урон репутации компании
5	Критический ущерб	Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным

дальнейшую деятельность организации

При использовании качественных шкал для вычисления уровня риска применяются специальные таблицы, в которых в первом столбце задаются понятийные уровни ущерба, а в первой строке - уровни вероятности атаки. Ячейки же таблицы, расположенные на пересечении первой строки и столбца, содержат уровень риска безопасности. Размерность таблицы зависит от количества концептуальных уровней вероятности атаки и ущерба. Пример таблицы, на основе которой можно определить уровень риска, приведён в табл. 3.3.

Таблица 3.2. Качественная шкала оценки вероятности проведения атаки

№	Уровень вероятности атаки	Описание
1	Очень низкая	Атака практически никогда не будет проведена. Уровень соответствует числовому интервалу вероятности [0, 0.25)
2	Низкая	Вероятность проведения атаки достаточно низкая. Уровень соответствует числовому интервалу вероятности [0.25, 0.5)
3	Средняя	Вероятность проведения атаки приблизительно равна 0,5
4	Высокая	Атака скорее всего будет проведена. Уровень соответствует числовому интервалу вероятности (0.5, 0.75]
5	Очень высокая	Атака почти наверняка будет проведена. Уровень соответствует числовому интервалу вероятности (0.75, 1]

Таблица 3.3. Пример таблицы определения уровня риска информационной безопасности

Вероятность атаки	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Ущерб					
Малый ущерб	Низкий Риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный ущерб	Низкий Риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Ущерб средней тяжести	Низкий Риск	Средний риск	Средний риск	Средний риск	Высокий риск
Большой ущерб	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск

Критический ущерб	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

При расчете значений вероятности проведения атаки, а также уровня возможного ущерба могут использоваться статистические методы, методы экспертных оценок или элементы теории принятия решений. Статистические методы предполагают анализ уже накопленных данных о реально случавшихся инцидентах, связанных с нарушением информационной безопасности. На основе результатов такого анализа строятся предположения о вероятности проведения атак и уровнях ущерба от них в других АС. Однако применение статистических методов не всегда возможно из-за отсутствия в полном объёме статистических данных о ранее проведённых атаках на информационные ресурсы АС, аналогичной той, которая выступает в качестве объекта оценки.

При использовании аппарата экспертных оценок проводится анализ результатов работы группы экспертов, компетентных в области информационной безопасности, которые на основе имеющегося у них опыта определяют количественные или качественные уровни риска. Элементы теории принятия решений позволяют применять для вычисления значения риска безопасности более сложные алгоритмы обработки результатов работы группы экспертов.

В процессе анализа рисков информационной безопасности могут использоваться специализированные программные комплексы, позволяющие автоматизировать процесс анализа исходных данных и расчёта значений рисков. Примерами таких комплексов являются "Гриф" и "Кондор" (компании "Digital Security"), британский CRAMM (компания Insight Consulting, подразделение Siemens), американский RiskWatch (компания RiskWatch), а также "АванГард" (Института Системного Анализа РАН).

Традиционно выделяют три основные составляющие безопасности информации:

конфиденциальность (confidentiality) - сохранение информации в тайне, невозможность раскрытия информации без согласия заинтересованных сторон;

целостность (integrity) - непротиворечивость и правильность информации, защита информации от неавторизованной модификации;

доступность (availability) - обеспечение наличия информации и работоспособности основных услуг для пользователя в нужное для него время.

Ведутся дискуссии на тему полноты " триады CIA " для описания угроз ИБ. Существует альтернатива этой классификации - т.н. " гексада Паркера " (Parkerian Hexad). Помимо вышеперечисленных свойств, Дон Паркер выделяет:

подлинность (authenticity) - в применении к пользователю определяет соответствие участника взаимодействия своему имени; в применении к сообщению - достоверность того, что данные были созданы заявленным источником.

управляемость, или владение (possession or control) - гарантия того, что законный владелец является единственным лицом, во власти которого изменить информацию или получить к ней доступ на чтение

полезность (utility) - "практичность", удобство доступа; нахождение информации в такой форме, что ее законный владелец не должен для получения доступа тратить неоправданных усилий (таких, как преобразование формата, подбор ключа шифрования и т.д.)

Существует также классификация 5A, горячо одобряемая известным криптографом Брюсом Шнайером:

Authentication (аутентификация: кто ты?)

Authorization (авторизация: что тебе можно делать?)

Availability (доступность: можно ли получить работать с данными?)

Authenticity (подлинность: не повреждены ли данные злоумышленником?)

Admissibility (допустимость: являются ли данные достоверными, актуальными и полезными?)

Мы в данном курсе будем придерживаться модели угроз STRIDE, являющейся компонентом используемой Microsoft методологии SDL (Secure Development Lifecycle).

Spoofing (притворство)

Tampering (изменение)

Repudiation (отказ от ответственности)

Information Disclosure (утечка данных)

Denial of Service (отказ в обслуживании)

Elevation of Privilege (захват привилегий)

Данная классификация расширяет традиционный подход к оценке безопасности информации (покрытие области CIA обеспечивают компоненты Tampering + Information Disclosure + Denial of Service) и позволяет разработчику взглянуть на информационную систему с позиции злоумышленника. Далее мы будем рассматривать продукты и технологии, упорядочивая их согласно тому, от какого типа угрозы по классификации STRIDE они призваны защитить информационные ресурсы.

Краткие итоги

В данной лекции были рассмотрены принципы применения анализа рисков для управления информационной безопасностью предприятия. Проведен сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, Гексада Паркера, 5A, STRIDE.

5.3 ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ СРЕДСТВ ОБЕСПЕЧЕНИЯ ПЕРСОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Экономическая эффективность средств обеспечения персональной кибербезопасности

Важность экономического обоснования инвестиций в ИБ подчеркивал В.Мамыкин, директор по информационной безопасности кабинета президента Microsoft в России и СНГ, в своих выступлениях на конференциях Security @ Interop '2008 и IT-Summit'2008 [7.48]. Согласно [7.49], большинство зарубежных компаний (84%) используют ROI и другие инструменты для оценки инвестиций в ИБ, которые составляют в среднем 5% всего ИТ-бюджета. В России на ИБ идет 0,5% ИТ бюджета, т.е. в 10 раз меньше. Такую ситуацию В.Мамыкин напрямую связывает с тем, что в нашей стране пока не получила широкого распространения практика оценки эффективности средств обеспечения ИБ с экономических позиций.

Расчет финансово-экономических показателей СЗИ позволяет решить следующие задачи [7.47]:

Обоснование внедрения системы по обеспечению информационной безопасности на предприятии с экономической точки зрения;

Оценка экономической эффективности внедрения или замены системы безопасности информации;

Прогнозирование расходов по созданию/ функционированию/ модернизации СЗИ (задача управления бюджетом);

Сравнение по экономическим критериям нескольких вариантов создания СЗИ, построенных на различных архитектурах (системах и компонентах), с целью выбора оптимального варианта реализации проекта (задача выбора ИТ-стратегии).

Качество информации, необходимой для принятия решения о целесообразности инвестиций, в первую очередь, будет зависеть от исходных данных, на основе которых производились вычисления. Уязвимым местом в любой методике расчета является именно сбор и обработка первичных данных, их качество и достоверность. Одним из основных вопросов является оценка затрат на ИБ. Выбор необходимой степени защиты должен учитывать ряд критериев: уровень секретности информации; ее стоимость; время, в течение которого она должна оставаться в тайне и т.д. Известный криптограф Брюс Шнайер (Bruce Schneier) в работе [7.26] подчеркивает, что термин "безопасность" лишен

смысла без сведений о том, от кого и на какой срок защищена информация. Это утверждение применимо как к системам обеспечения безопасности в целом, так и к их важнейшему компоненту - средствам криптографической защиты информации.

Средства криптографической защиты информации (СКЗИ) представляют собой средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности. Росс Андерсон (Ross J Anderson), ведущий эксперт в области информационной безопасности, в своей статье [7.3] приходит к выводу, что при оценке уровня защищенности специалист должен принимать во внимание не только технические характеристикикриптосистемы, получаемые путем криптоанализа и анализа информационных потоков, но использовать также и экономические инструменты.

Рассмотрим возможность разработки методики анализа эффективности СКЗИ с учетом того, каким угрозам защищаемая информация будет подвергаться со стороны злоумышленников.

Для решения поставленной задачи необходимо:

формализовать процесс оценки эффективности криптографической защиты;

разработать математическую модель угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств;

обеспечить криптоаналитика набором инструментальных средств, позволяющих оценить стойкость криптографических средств по отношению к идентифицированным угрозам;

провести анализ существующих методов оценки СКЗИ с экономических позиций и выбрать финансово-экономические показатели, подходящие для экономической оценки инвестиций в СКЗИ.

Поставленные цели согласуются с задачами, вошедшими в перечень основных направлений и приоритетных проблем научных исследований в области информационной безопасности Российской Федерации, который был разработан секцией по информационной безопасности Научного совета при Совете Безопасности Российской Федерации при активном участии ведущих ученых и специалистов научных учреждений и организаций РАН, вузов, федеральных органов исполнительной власти, работающих в различных областях, связанных с обеспечением национальной безопасности (см. [7.44], пп. 46, 47 и 56).

Процесс оценки эффективности криптографической защиты

Анализ существующих подходов

При оценке эффективности СКЗИ важнейшим критерием считается криптостойкость, т.е. способность противостоять атакам криптоаналитика [7.40]. Такой подход не учитывает других важных требований к криптосистемам, а именно (см. [7.46]):

минимальный объем используемой ключевой информации;

минимальная сложность реализации (в количестве машинных операций);

стоимость;

высокое быстродействие.

Кроме того, использование СКЗИ, обеспечивающих устойчивость к взлому ниже некоторой "фоновой" вероятности, является экономически неоправданным [7.35]. Например, если вероятность выхода компании из бизнеса равна 230 (менее чем один из миллиона), то есть ли смысл для защиты информации, которая может нанести компании ущерб, сопоставимый с кризисом рынка, использовать алгоритм, вероятность вскрытия которого за приемлемое время составляет 2100?

В статье В.П.Иванова [7.38] эффективность криптографических средств защиты предлагается оценивать с использованием математического аппарата теории массового обслуживания и теории катастроф на основе вероятностно-временной группы показателей, в числе которых:

среднее время безопасного функционирования защищаемой системы;

время безопасного функционирования защищаемой системы с вероятностью НСД не выше заданной;

экономическая эффективность созданной системы защиты информации.

Выбор показателей эффективности представляет интерес, однако методика имеет ряд критических недостатков, которые делают невозможным ее применение на практике для оценки современных СКЗИ. В первую очередь это границы применимости: методика подходит только для оценки криптосистем, принадлежащих по классификации Ж.Брассара (Gilles Brassard) [7.6] к классу криптосистем ограниченного использования, стойкость которых основывается на сохранении в секрете алгоритмов зашифрования и расшифрования. Однако, согласно фундаментальному допущению Кирхгоффа (Auguste Kerckhoffs) [7.14], стойкость криптосистемы должна основываться не на секретности алгоритмов зашифрования и расшифрования, а на секретности некоторого значения, которое называется ее ключом. Все современные криптосистемы построены по этому принципу, и исследования их надежности всегда должны проводиться в предположении, что потенциальному противнику о криптосистеме известно все, за исключением используемого ключа.

Еще одним недостатком методики, описанной в работе [7.38], является то, что она не учитывает зависимости эффективности криптосистемы от условий ее использования. Очевидно, эффективность одной и той же криптосистемы в разных контекстах может существенно отличаться, т.к. среда функционирования системы накладывает определенные ограничения на возможные сценарии атак.

Существуют методики, позволяющие построить модели угроз и уязвимостейинформационных систем и на основе анализа рисков получить количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты (см., например, [7.39]):

метод CRAMM, разработанный Агентством по компьютерам и телекоммуникациям Великобритании по заданию Британского правительства [7.9];

семейство программных продуктовRiskWatch от одноименной американской компании [7.23];

комплексная система анализа и управления рискамиинформационной системы ГРИФ, созданная отечественной компанией Digital Security [7.10].

Эти инструментальные средства полезны специалисту при проведении аудита систем обеспечения безопасности предприятия, однако они не учитывают специфики СКЗИ и, как показано в [7.34], не подходят для решения поставленной в данной работе задачи.

Наконец, существуют методы формального анализа криптопротоколов. Криптографический протокол [7.24] регламентирует последовательность действий, выполняемых двумя и более сторонами для решения какой-либо задачи с использованием криптографических преобразований и алгоритмов. Можно выделить три основных класса методов анализа криптопротоколов:

Дедуктивные методы, основанные на автоматическом доказательстве теорем, связанных со свойствами исследуемого криптопротокола [7.5];

Методы анализа состояний, моделирующие криптопротокол в виде конечного автомата [7.4];

Методы статического анализа, объектом исследования в которых являются потоки данных и управления [7.7].

Перечисленные подходы имеют существенный недостаток: все они построены на предположении, что используемые в протоколе криптографические примитивы идеальны. Рассматривается только концептуальная схема протокола, от конкретных методов шифрования и их подверженности атакамзлоумышленника принято абстрагироваться.

Модель процесса оценки эффективности СКЗИ

Наиболее эффективным при выборе и оценке криптографической системы считается использование экспертных оценок [7.46]. При оценке эффективности СКЗИ необходимо принимать во внимание взаимосвязь факторов, определяющих ее подверженность атаке определенного типа. Упрощенное графическое представление модели сценария атаки изображено на рис. 7.1. Во избежание избыточности из модели исключен элемент "Защищаемые ресурсы", который задается неявно - через элемент "Злоумышленник" (характер зашифрованной информации определяет возможных злоумышленников, которые могут осуществлять попытки взлома в целях нарушения конфиденциальности, целостности или доступности).

Рис. 7.1. Модель сценария взлома

На основании предложенной модели сценария атаки построена модель угроз безопасности информационных ресурсов из трех элементов [7.30] - ABC-модель ("A" от англ. Attack - атака, "B" от англ. code-Breaker - взломщик шифра, "C" от англ. Cryptosystem - криптосистема). Математическое описание ABC -модели дано позже, здесь мы рассмотрим процесс экспертной оценки эффективности криптографической защиты (графическая модель процесса изображена на рис. 7.2).

Целью этапов 1-3 является построение ABC -модели. Первый этап - определение объекта исследования. Здесь описываются конкретные характеристики криптосистемы. На втором этапе задаются параметры, определяющие тип потенциальных взломщиков криптосистемы. Как будет показано в следующем разделе, при наличии формальных представлений исследуемой криптосистемы и потенциальных злоумышленников мы можем перейти к третьему этапу, т.е. определить типы атак, которым подвержена криптосистема, а также связанный с ними риск.

Четвертый этап представляет собой анализ устойчивостикриптосистемы к атакам, определенным на третьем этапе. Для проведения криптоанализа специалиста необходимо обеспечить набором инструментальных средств, исследование и разработке которых будет рассмотрена далее.

Наконец, пятый этап предполагает использование различных подходов к оценке экономической эффективности инвестиций в СКЗИ на основании данных, полученных на этапах 1-4.

Рис. 7.2. Процесс оценки эффективности криптографической защиты

Моделирование угроз безопасности информационных ресурсов

Задача состоит в разработке АВС -модели угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств, которая даст возможность формализовать взаимосвязь между параметрами криптосистемы, потенциальных злоумышленников и возможных атак. Для решения поставленной задачи необходимо:

Разработать многокритериальные классификационные схемы, позволяющие идентифицировать:

криптосистему - с учетом особенностей ее реализации;

потенциального взломщика - с учетом его мотивации, возможностей и квалификации;

криптоаналитическую атаку - с учетом применимости к различным криптосистемам и необходимых для ее осуществления ресурсов.

На основе разработанных классификаций создать параметрические модели криптосистем, атак и злоумышленников;

Установить зависимость возможных сценариев взлома от характеристик злоумышленников и от особенностей реализации исследуемой криптосистемы.

Анализ существующих подходов

Для идентификации исследуемой криптосистемы нужно выделить набор ее ключевых свойств. Известны классификации криптосистем, в числе которых - классификационная схема, предложенная швейцарским математиком и криптографом У.Маурером (Ueli Maurer) [7.21] и основанная на том, чтобы различать криптосистемы по количеству ключей, упомянутая выше схема Ж.Брассара [7.6], в которой криптосистемы различаются в зависимости от сохранения в секрете механизма шифрования. Ни одна из этих классификаций сама по себе не позволит идентифицироватькриптосистему - необходима многокритериальная классификация. С этой точки зрения представляет интерес работа К.Черезова [7.43], в которой предлагаются обобщающие критерии для сравнения продуктов на российском рынке СКЗИ:

Фирма-производитель;

Тип реализации;

Наличие действующих сертификатов соответствия ФСБ России и классы защиты;

Реализованные криптографические алгоритмы;

Поддерживаемые операционные системы;

Предоставляемый программный интерфейс;

Наличие реализации протокола SSL / TLS ;

Поддерживаемые типы ключевых носителей;

Интегрированность с продуктами и решениями компании Microsoft ;

Наличие дистрибутива продукта в свободном доступе на сайте производителя, дилерской сети распространения и сервиса поддержки.

Недостатком приведенной классификации для построения параметрической модели криптосистемы является то, что для решения поставленной в нашей работе задачи важны не "потребительские" и "технические" характеристики СКЗИ, а их свойства, определяющие подверженность тем или иным атакам.

Типы взломщиков, от которых криптосистема должна обеспечить защиту, определяют разумный уровень безопасности. Чтобы понять, каким атакам будет подвергаться система, необходимо выделить наиболее вероятных взломщиков. Классификации Дж.Говарда (John D Howard) [7.13] и Б.Шнайера [7.25], в которых злоумышленники различаются в зависимости от их движущих мотивов, подходят для высокоуровневого анализа контекста использования криптосистемы, однако не позволяют установить зависимость возможных сценариев атак от характеристик злоумышленников.

Существует большое количество классификаций и таксономийатак. Недостатком схем, описанных в [7.15, 7.17, 7.22, 7.28], является то, что они разработаны для описания атак на компьютерные системы, а объектом нашего исследования является более узкий класс атак - криптоаналитические атаки. Классификация Кирхгоффа [7.14] по доступу к открытому и зашифрованному тексту с появлением атак по побочным каналам [7.37] уже не может считаться полной; кроме того, она не позволяет учитывать такие важные факторы, как объем необходимых ресурсов, возможность распараллеливания и т.д.

Математическая модель угроз безопасности информационных ресурсов

На основе анализа существующих классификационных схем, перечисленных выше, нами были разработаны новые многокритериальные классификации криптосистем, атак и злоумышленников (см. рис. 7.3 - 7.5). Далее мы покажем, как применение разработанных классификационных схем для построения ABC -модели позволяет провести всесторонний анализ угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств.

Пусть $A \subseteq A_1 \times A_2 \times \ldots \times A_8$- множество параметрических моделей атак, где A_i($i = \overline{1,9}$) - множество значений i-го параметра модели атаки, определяющего тип атаки в соответствии с критериями разработанной классификации. Каждая модель $\vec{a} \in A$ представляет собой вектор $(a_1, a_2, \ldots, a_9)$, где $\vec{a_i} \in A_i$.

Аналогично, параметрическая модель злоумышленника задается в виде вектора $\vec{b} \in B$, где $B \subseteq B_1 \times B_2 \times \ldots \times B_6$, B_j($j = \overline{1,6}$) - множество значений j-го параметра модели злоумышленника, модель криптосистемы - $\vec{c} \in C$, где $C \subseteq C_1 \times C_2 \times \ldots \times C_6, C_k$($k = \overline{1,6}$) - множество значений k-го параметра модели криптосистемы в соответствии с многокритериальной классификацией. Заметим, что множества значений параметров модели атаки, злоумышленника и криптосистемы конечны.

При дальнейшем изложении для краткости слово "модель" применительно к модели атаки, модели злоумышленника и модели криптосистемы будем опускать.

С каждой атакой будем связывать значение риска, вычисляемое по общеизвестной формуле на основе двух факторов - вероятности происшествия и тяжести возможных последствий:

Риск = Влияние Вероятность

Обозначим через $\Re : A \times B \times C \to [0;1]$функцию, задающую уровень риска, связанного с атакой $\vec{a} \in A$ в условиях, когда она может быть применена злоумышленником $\vec{b} \in B$ для взлома криптосистемы $\vec{c} \in C$.

Пусть $I : C \times A \to [0;1]$- функция влияния (от англ. impact - влияние, воздействие). Под влиянием мы будем понимать степень ущерба от применения атаки $\vec{a} \in A$ к криптосистеме $\vec{c} \in C$.

Пусть $P : B \times A \to [0;1]$- вероятность того, что злоумышленник $\vec{b} \in B$ предпримет атаку $\vec{a} \in A$, т.е. обладает ресурсами для ее осуществления и сочтет эту атаку целесообразной.

Тогда функция риска $\Re$ выражается следующим образом:

$$\Re(\vec{a}, \vec{b}, \vec{c}) = I(\vec{c}, \vec{a}) * P(\vec{b}, \vec{a})$$

Определим функцию $I(\vec{c}, \vec{a})$. Для этого рассмотрим семейство функций $I_{gh} : C_g \times A_h \to R_+$, , , где R_+- множество неотрицательных действительных чисел. Здесь функция I_{gh} задает уровень взаимного влияния параметра криптосистемы C_g и параметра атаки a_h:

$I_{gh}(c, a) = 0$, если атака со значением параметра $a \in A_h$ не применима к криптосистеме со значением параметра $c \in C_g$;

$0 < I_{gh}(c, a) < 1$, если значение параметра криптосистемы $c \in C_g$ снижает вероятность успешного применения атаки со значением параметра $a \in A_h$;

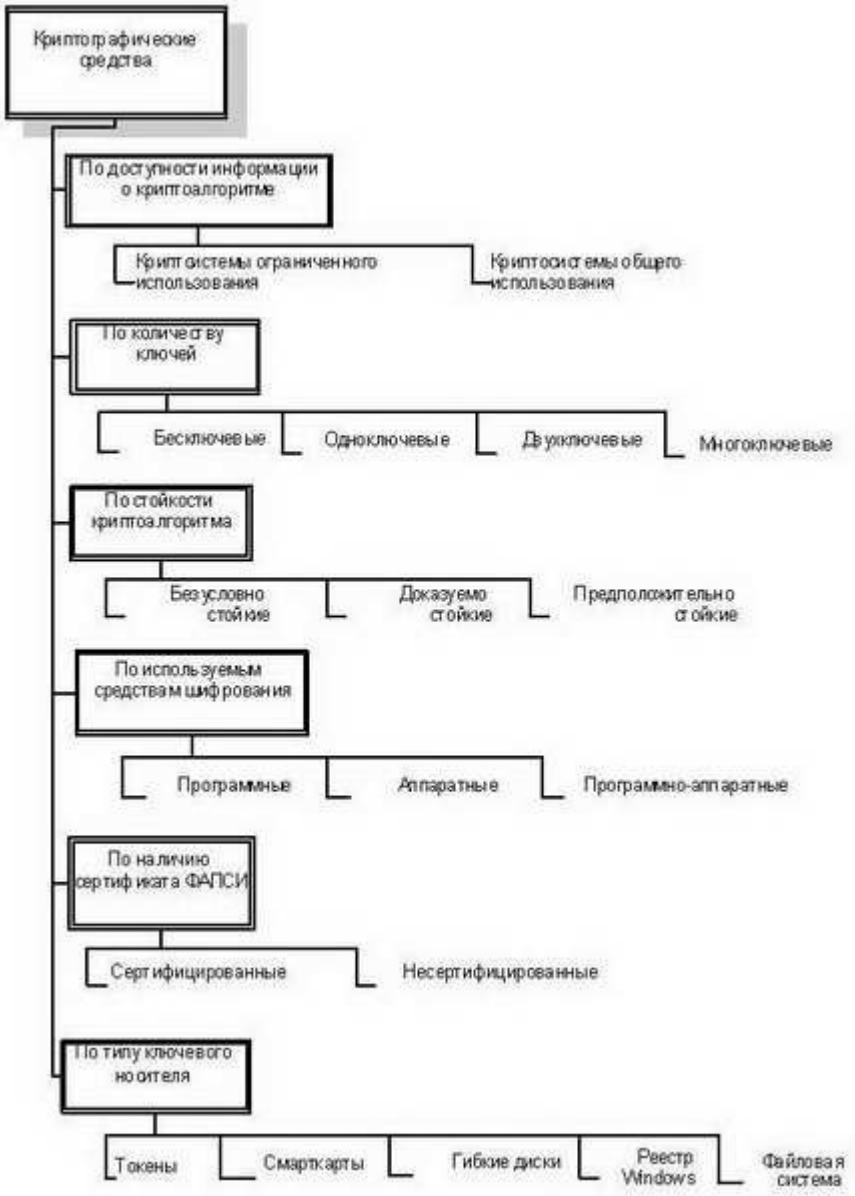

Рис. 7.3. Классификация криптосистем

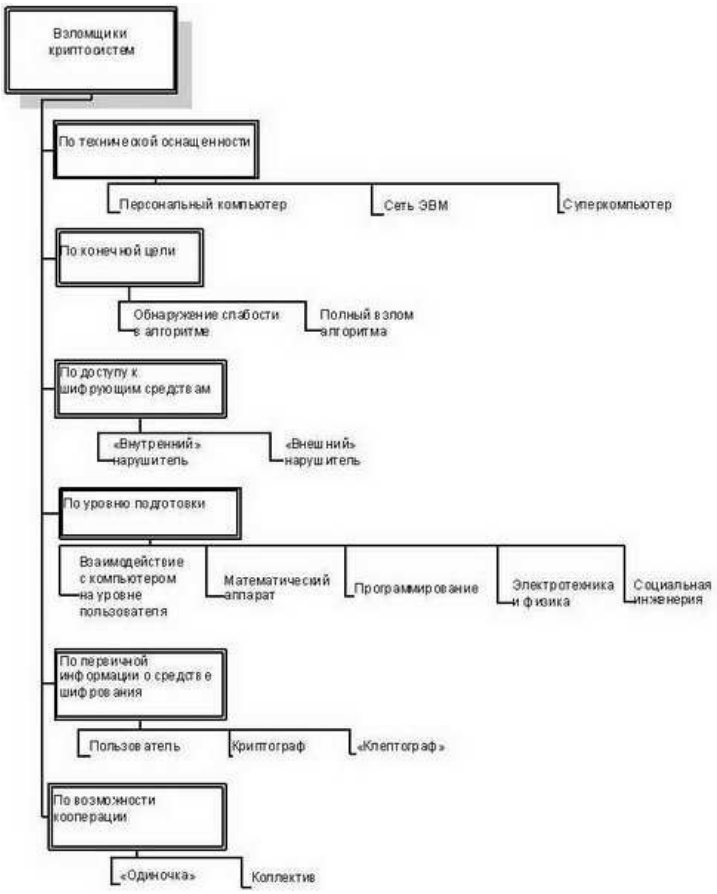

Рис. 7.4. Классификация злоумышленников

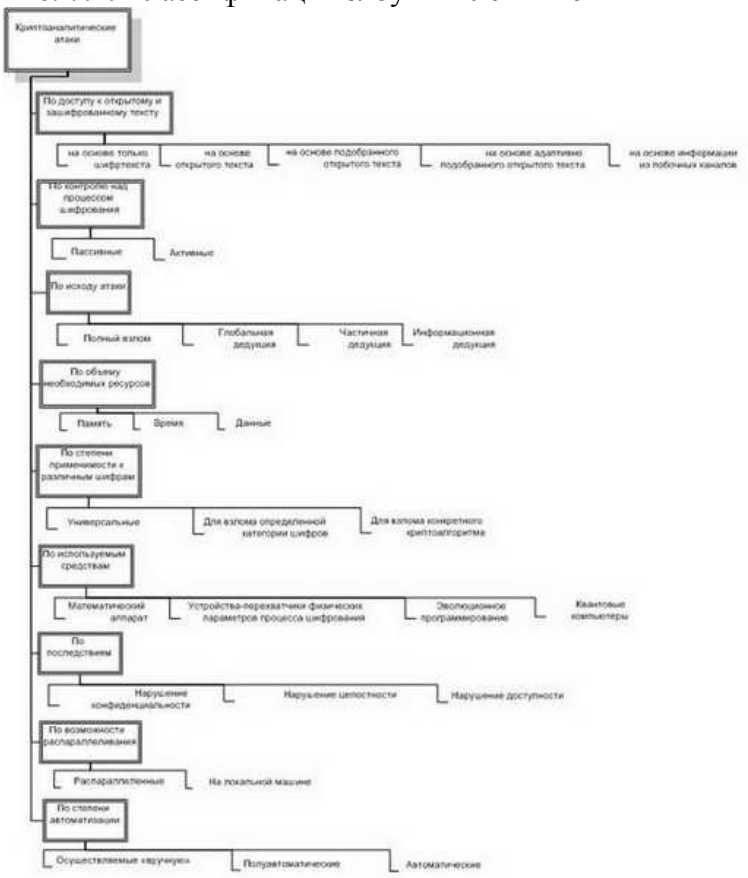

Рис. 7.5. Классификация криптоатак

$I_{gh}(c,a)=1$, если значение параметра криптосистемы $c \in C_g$ не влияет на применимость атаки с параметром $a \in A_h$;

$I_{gh}(c,a)>1$, если значение параметра криптосистемы $c \in C_g$ указывает на то, что атака с параметром $a \in A_h$ применима для ее взлома.

Например, если исследуемый алгоритм шифрования реализован в аппаратном обеспечении, это повышает вероятность применения для взлома криптосистемыатак по побочным каналам [7.37] (это вид криптографических атак, использующих информацию, которая может быть получена с устройства шифрования и не является при этом ни открытым текстом, ни шифртекстом). Уровень взаимного влияния параметров криптосистемы и атаки определяется на основе экспертных оценок.

Обозначим через $\overline{I_{gh}} : C_g \times A_h \to [0;1]$ нормированную функцию:

$$\overline{I_{gh}}(c,a)=\frac{I_{gh}(c,a)}{\sum_{\xi \in C_g} I_{gh}(\xi,a)}$$

Тогда уровень ущерба от применения атаки $\vec{a} \in A$ к криптосистеме $\vec{c} \in C$ вычисляется по следующей формуле:

$$I(\vec{c},\vec{a})=\min_{h=\overline{1,9}} \prod_{g=\overline{1,6}} \overline{I_{gh}}(c_g,a_h)$$

,

где атака и криптосистема заданы параметрами $(a_1,a_2,\ldots,a_9)$ и $(c_1,c_2,\ldots,c_6)$ соответственно. Заметим, что уровень влияния всех параметров криптосистемы на применимость атаки с заданным значением -го параметра в этой формуле вычисляется по мультипликативному критерию: $\prod_{g=1}^{6} \overline{I_{gh}}(c_g,a_h)$. Если значение хотя бы одного из параметров криптосистемы противоречит возможности применения атаки, то результатом оценки применимости атаки к криптосистеме будет нулевое значение, что соответствует нулевому уровню ущерба от атаки.

Функция $P(\vec{b},\vec{a})$, определяющая зависимость между параметрами $(a_1,a_2,\ldots,a_9)$ атаки и $(b_1,b_2,\ldots,b_6)$ злоумышленника, выражается аналогично функции $I(\vec{c},\vec{a})$. В качестве иллюстрации взаимосвязи параметров злоумышленника и атаки можно привести следующий пример: наличие у предполагаемого взломщика доступа к распределенным вычислительным ресурсам повышает вероятность применения метода "грубой силы" и, вообще говоря, любой атаки, легко поддающейся распараллеливанию.

Таким образом, общая формула для определения уровня риска, связанного с атакой $\vec{a} \in A$ в условиях, когда эта атака может быть применена злоумышленником $\vec{b} \in B$ для взлома криптосистемы $\vec{c} \in C$, имеет вид:

$$\Re(\vec{a},\vec{b},\vec{c})=\min_{h=\overline{1,9}} \prod_{g=\overline{1,6}} \overline{I_{gh}}(c_g,a_h) * \min_{h=\overline{1,9}} \prod_{t=\overline{1,6}} \overline{P_{th}}(b_t,a_h)$$

Будем считать, что криптосистема $\vec{c} \in C$ подвержена атаке $\vec{a} \in A$ в условиях, когда ей угрожает злоумышленник $\vec{b} \in B$, если $\Re(\vec{a}, \vec{b}, \vec{c}) > \theta$, т.е. связанный с ней уровень риска превышает заданное пороговое значение θ, где $\theta \in [0;1]$. Допустимый уровень риска θ является настраиваемым параметром ABC -модели угрозкриптосистемы. Значение θ задается с учетом двух критериев:

критичности защищаемых данных;

временных и других ресурсов, доступных специалисту, который осуществляет аудит системы.

В общем случае:

криптосистема может включать несколько подсистем (например, генератор ключей и симметричныйшифратор), к каждой из которых применим свой набор атак;

на криптосистему может нападать несколько злоумышленников.

Множество атак, которым подвержена криптосистема, состоящая из подсистем $\vec{c} \in C'$ ($C' \subseteq C$), в условиях, когда ей угрожают злоумышленники $\vec{b} \in B'$ ($B' \subseteq B$), будем определять по формуле $\Lambda = \bigcup_{\vec{b} \in B'} \bigcup_{\vec{c} \in C'} \lambda(\vec{b}, \vec{c})$, где $\lambda(\vec{b}, \vec{c}) = \{\vec{a} \in A : \Re(\vec{a}, \vec{b}, \vec{c}) > \theta\}$ при заданном уровне риска. Для оценки защищенности криптосистемы необходимо с использованием инструментальных средств оценить ее способность противостоять атакам, входящим в множество Λ.

В описанной математической модели сделаны следующие допущения:

не учитывается зависимость параметров атаки от сочетания параметров криптосистемы, хотя влияние каждого параметра принимается во внимание;

не учитывается возможность совместных действий со стороны взломщиков различных типов, хотя можно задать модель нападения со стороны однородного коллектива злоумышленников.

Исправление ABC -модели с учетом указанных допущений привело бы к ее значительному усложнению. Вопрос о том, насколько эти допущения снижают точность моделирования угроз безопасности, подлежит дальнейшим исследованиям.

Важно отметить, что разработанная классификационная схема для построения моделей атак на алгоритмы шифрования с небольшими модификациями применима и для моделирования атак на криптопротоколы. Возможность использования ABC -модели угроз для комплексного исследования криптосистемы является важной, т.к. вопрос совместного функционирования криптопротоколов и шифров в рамках одной криптосистемы, как показано в [7.27], до сих пор был мало изучен.

Оценка стойкости криптографических средств к идентифицированным угрозам

После того, как выделен набор атак, представляющих наибольшую угрозу для защищаемых данных, необходимо оценить способность криптосистемы противостоять этим атакам.

Базой для получения таких оценок может служить статистика взлома и успешных атак на криптосистемы. Например, известно, что стартовавший в 1997 г. на сайте www.distributed.net проект "распределенного взлома" RC5-64 (блочного шифра компании RSA, использующего 64-битный ключ) [7.29], в котором на добровольной основе приняли участие более 300 тысяч пользователей глобальной сети, был успешно завершен за пять лет (1757 дней) - за это время было перебрано 85% всего пространства ключей. Однако такая информация, во-первых, не всегда доступна, а, во-вторых, со временем теряет актуальность, т.к. повышение производительности вычислительной техники и появление новых видов атак на шифры ведет к понижению стойкости известных криптографических алгоритмов. Для проверки надежности шифров, используемых в криптосистеме, специалисту необходим набор инструментальных средств, позволяющих осуществлять

криптоанализ и не предполагающих у использующего их специалиста наличия глубоких знаний в программировании или электротехнике. В качестве примера можно привести упомянутые в п.1.1 автоматизированные средства анализа криптопротоколов [7.7] или прототип программного комплекса для моделирования атак по побочным каналам [7.37], описанный в [7.19]. Моделирование аппаратного обеспечения в работе [7.19 осуществляется с использованием SystemC [7.2] - языка проектирования и верификации моделей системного уровня, реализованного в виде библиотеки на C++ с открытым исходным кодом. На примере программных и аппаратных реализаций шифраAES показано, каким образом разработанный инструмент позволяет обнаружить уязвимости в реализации криптографического алгоритма.

Особого внимания заслуживают асимметричные криптосистемы. Функциональные возможности шифров с открытым ключом используются в разнообразных технологиях, в числе которых [7.33]:

Управление идентичностью;

Цифровая подпись кода;

Доверенная платформа;

Управление авторством;

Построение VPN ;

Гарантированное уничтожение информации;

Защита от физической кражи носителя информации.

Процесс криптоанализа асимметричных шифров сопряжен с решением задач из теории чисел и общей алгебры, т.к. практически все используемые алгоритмы асимметричной криптографии основаны проблемах факторизации и дискретного логарифмирования в различных алгебраических структурах. Чтобы определить, могут ли математические задачи той или иной размерности считаться достаточно прочным фундаментом для криптографических целей, специалисту требуются инструментальные средства, позволяющие оценивать быстродействие алгоритмов факторизации и дискретного логарифмирования. Необходимо учитывать, что криптоаналитик может не обладать навыками в области программирования. Кроме того, важно предусмотреть возможность работы под управлением наиболее распространенной ОС - MS Windows.

Итак, выделим набор основных требований к инструментальным средствам криптоанализа:

Эффективность вычислений с длинными числами в модулярной арифметике;

Наличие алгоритмов работы с разреженными матрицами;

Наличие алгоритмов создания факторной базы, решета и разложения на множители;

Удобство пользовательского интерфейса;

Возможность сборки в ОС Windows.

Будем считать, что решение соответствует поставленной задаче, если оно удовлетворяет всем перечисленным пяти критериям оценки.

Анализ существующих подходов

Математические пакеты Maple [7.36] и Mathematica [7.45] отличаются простотой кодирования алгоритмов и не имеют встроенных ограничений на разрядность операндов. Тем не менее, помимо платформенной зависимости они обладают критическим недостатком - низкой эффективностью теоретико-числовых операций.

Высокой эффективности можно добиться, используя встроенные средства низкоуровневого языка программирования для разработки функций, необходимых для исследования криптосистем. Однако важно отметить, что реализация примитивов для конструирования современных методов криптоанализа асимметричных шифров оперирует числами в длинной арифметике. Встроенные числовые типы языков C и C++ имеют ограниченную разрядность:

long: 32 бита;

long long: 64 бита;

double: 53 бита - мантисса, 11 бит - экспонента;

long double: в зависимости от реализации языка может быть определен как double (см. выше) либо как extended double: 64 бита - мантисса, 15 бит - экспонента [7.1].

В реализации языков на платформе . NET отсутствует тип extended double: он доступен только неявно при выполнении промежуточных вычислений (например, где умножение дает результат, выходящий за пределы диапазона значений double, но последующее деление возвращает промежуточный результат обратно в этот диапазон). Кроме того, существует встроенный 128-битный тип данныхdecimal, позволяющий представлять целые числа разрядностью до 96 бит (в соответствии с размером мантиссы), однако он реализуется в режиме эмуляции, поскольку аппаратная поддержка этого типа на сегодняшний день отсутствует [7.11].

Java поддерживает возможность работы с длинными числами и обладает переносимостью, однако недостатком является низкая эффективность реализации.

Рассмотрим специализированные библиотеки функций для работы с длинной арифметикой и теоретико-числовыми задачами, находящиеся в открытом доступе: LIP, LiDIA, CLN, GMP, NTL.

Библиотека для работы с длинной арифметикойLIP (Long Integer Package) [7.18] является одной из первых таких библиотек. Она была разработана на языке ANSIC известным специалистом Арженом Ленстрой (Arjen K. Lenstra) и поддерживается Полом Лейлендом (Paul Leyland). При хорошей переносимости эта библиотека обладает низкой эффективностью. Кроме того, в ней отсутствует поддержка высокоуровневых теоретико-числовых алгоритмов.

Библиотека CLN (a Class Library for Numbers) [7.8] реализует элементарные арифметические, логические и трансцендентные функции. Авторами библиотеки являются Бруно Хейбл (Bruno Haible) и Ричард Крекел (Richard Kreckel). CLN содержит большой набор классов, реализованных на C++, в частности, классы для поддержки модулярной арифметики, операций с целыми, рациональными и комплексными числами, числами с плавающей запятой. Поскольку числовая библиотека задумывалась как универсальная, это привело к ее ограниченной применимости для решения узкоспециализированных задач.

Библиотека теоретико-числовых алгоритмов LiDIA [7.16], предложенная Томасом Папаниколау (Thomas Papanikolau, Technical University of Darmstadt), написана на C++,поддерживает различные пакеты для работы с целыми числами (GMP, CLN, LIP) и характеризуется высокоэффективными реализациями типов данных с увеличенной точностью и алгоритмов с большой временной сложностью. Недостатком библиотеки LiDIA является невозможность сборки в операционных системах Windows, что очень существенно в связи с широким использованием продуктов Microsoft и необходимостью проверки их защищенности.

При разработке GMP (GNU Multiple Precision arithmetic library) [7.12] был сделан упор на скорость. Эффективность от использования библиотеки теоретико-числовых алгоритмов GMP растет при увеличении разрядностиоперандов. Часть функций реализована на языке C, часть - на ассемблере. Автором является Торбжорд Гранланд (Torbjord Granlund). Помимо несовместимости с платформой Windows, недостатком GMP является отсутствие алгоритмов формирования факторной базы, разложения на множители и ряда других, необходимых для реализации современных методов криптоанализа.

Таблица 7.1. Сравнительный анализ программных решений для решения задач криптоанализа

Решение	Mathematica	LIP	CLN	LiDIA	GMP	NTL	КРИПТО

Критерии оценки							
Эффективность вычислений	-	-	-	+	+	+	+
Возможность сборки в ОС Windows	+	+	+	-	-	+	+
Наличие алгоритмов работы с разреженными матрицами	-	-	-	+	+	-	+
Наличие алгоритмов создания факторной базы, решета и разложения на множители	-	-	-	+	-	-	+
Удобство пользовательского интерфейса	+	-	-	-	-	-	+

Известная математическая библиотека библиотека NTL (a Library for doing Number Theory) [7.20] разработана Виктором Шаупом (Victor Shoup) для поддержки теоретико-числовых алгоритмов. Функции, реализованные на языке C++,характеризуются переносимостью. Библиотеку можно использовать совместно с GMP в целях повышения эффективности. NTL имеет большое количество преимуществ по сравнению с рассмотренными аналогами (см. табл. 7.1), однако для решения поставленной задачи реализованных в библиотеке NTL алгоритмов недостаточно. Кроме того, для ее использования в криптоанализе специалист должен обладать квалификацией программиста.

Как видно из табл. 7.1, ни одно из рассмотренных решений не удовлетворяет одновременно всем пяти установленным критериям.

Инструментальные средства криптоанализа асимметричных шифров

Для оценки стойкости криптосистем аналитику необходим инструмент, эффективно работающий с теоретико-числовыми задачами, обладающий простым пользовательским интерфейсом и легко расширяемый. Прототип такого средства для криптоанализа систем с открытым ключом реализован в виде программного комплекса "Инструментальные средства криптоанализа асимметричных шифров" (обозначение в таблице - КРИПТО) [7.31, 7.32]. Программный комплекс состоит из библиотеки КОНСТРУКТОР, включающей необходимые примитивы для конструирования современных методов криптоанализа асимметричных шифров, и приложения АНАЛИТИК, имеющего графический интерфейс пользователя для доступа алгоритмам факторизации и дискретного логарифмирования с использованием функций библиотеки КОНСТРУКТОР. Библиотека КОНСТРУКТОР написана на языке C++ и содержит компоненты, реализующие следующие основные функции:

Дискретное логарифмирование;

Факторизация целых чисел;

Тестирование чисел на простоту;

Решение систем линейных уравнений в кольцах вычетов и конечных полях.

Для выполнения операций с длинными числами использована библиотека NTL. Выбор базовой библиотеки, обусловленный её функциональностью, скоростью, компактностью (исходный код занимает чуть более 600 килобайт) и переносимостью, позволил получить эффективные реализации перечисленных теоретико-числовых алгоритмов. В настоящей работе мы не будем приводить полное сравнение библиотеки КОНСТРУКТОР с аналогами; заметим лишь, что если на решение задачи дискретного логарифмирования размерностью 55 бит с использованием системы Maple уходит порядка

8 часов, то разработанный программный комплекс КРИПТО позволяет за 10 минут вычислить дискретный логарифм в поле разрядностью 80 бит (испытания проводились на компьютере со следующими аппаратными характеристиками: процессор Intel Pentium IV 3,20GHz, ОЗУ 1Гб).

Расчет эффективности капитальных вложений в использование криптографических средств

Оценки вероятности взлома криптосистемы за определенный период позволяют определить сокращение риска НСД к данным от использования криптосистемы, например, за 1-й год - на 95%, за 2-й год - на 70%, за 3-й год - на 35%. При наличии достоверных оценок объема потерь от реализации угроз нарушения конфиденциальности, целостности или доступности защищаемых данных можно получить математические ожидания потерь и использовать их для определения эффективности криптосистемы с экономических позиций.

Анализ существующих подходов

В настоящее время нет единых стандартов, позволяющих оценить СКЗИ с экономических позиций, поэтому любой из разработанных методов заслуживает отдельного рассмотрения с выявлением его положительных и отрицательных сторон, а также сравнения его с другими представителями этого класса. В табл. 7.2 представлены результаты сравнительного анализа методов оценки эффективности инвестиций в средства обеспечения ИБ. На основании результатов был сделан вывод, что оптимальным является метод дисконтирования денежных потоков [7.42], позволяющий получить наиболее полное представление о целесообразности капитальных вложений, хотя и требующий много времени и усилий на расчет экономических показателей.

Методика дисконтирования денежных потоков при оценке эффективности инвестиций в СКЗИ

Определим денежные потоки, связанные с использованием СКЗИ, за период t (где t = 0, 1, 2…. T - периоды, T - горизонт расчета).

С защищаемой информацией связаны значения дохода $Profit_t$ от ее использования и ущерба $Loss_t$ от НСД в течение указанного промежутка времени t. Затраты $Cost_t$ на приобретение, установку и эксплуатацию СКЗИ могут быть определены очень точно. Пусть результаты оценки способности криптосистемы противостоять атакам показали, что в t-м периоде злоумышленник получит доступ к защищаемой информации с вероятностью P_t. Тогда математическое ожидание дохода R_t, связанного с использованием оцениваемой СКЗИ, вычисляется по формуле:

$$R_t = -Cost_t + Profit_t * (1 - P_t) - Loss_t * P_t$$

На основании этих данных о притоках и оттоках денежных средств вычисляются финансово-экономические показатели эффективности инвестиций в криптосистему и делаются выводы о ее соответствии потребностям организации.

Таблица 7.2. Сравнительный анализ методов оценки эффективности инвестиций в средства обеспечения ИБ

Методика оценки	Преимущества	Недостатки
Коэффициент возврата инвестиций	Показатель, понятный финансистам.	Отсутствие достоверных методов расчета в области ИТ. "Статичный" показатель.
Совокупная стоимость	Позволяет оценить целесообразность	Не учитывает качество

владения	реализации проекта на основании оценки только затрат. Предполагает оценку затрат на различных этапах всего жизненного цикла системы.	системы безопасности. "Статичный" показатель. Показатель, специфичный для ИТ.
Дисконтированные показатели эффективности инвестиций	Показатель, понятный финансистам. Учитывает зависимость потока денежных средств от времени. Учитывает все потоки денежных средств, связанные с реализацией проекта.	Сложность расчета.

Краткие итоги

Выполнен анализ существующих методов и средств оценки криптосистем, показаны их недостатки. Описаны этапы комплексного процесса оценки эффективности криптографических средств. Рассмотрены многокритериальные классификации криптосистем, атак и злоумышленников, положенные в основу их параметрических моделей. Описана математическая модельугроз безопасности информационных ресурсов, защищенных с использованием СКЗИ. Проведен сравнительный анализ программных средств, позволяющих решать задачи криптоанализа асимметричных шифров, показаны их преимущества и недостатки. Показаны преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения ИБ. Выделен набор финансово-экономических показателей для оценки эффективности СКЗИ с экономических позиций. Предложена методика дисконтирования денежных потоков при оценке эффективности инвестиций в СКЗИ.

5.4 ИНСТРУМЕНТЫ ОРГАНИЗАЦИИ ПЕРСОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Инструменты организации персональной кибербезопасности

Криптоалгоритмы с секретным ключом

Идея, лежащая в основе большинства итерационных блочных шифров, состоит в построении криптографически стойкой системы путем последовательного применения относительно простых криптографических преобразований. Принцип многоразового шифрования с помощью простых криптографических преобразований был впервые предложен Шенноном в работе [5.1]: он использовал с этой целью преобразования перестановки и подстановки. Первое из этих преобразований переставляет отдельные символы преобразуемого информационного блока, а второе - заменяет каждый символ (или группу символов) из преобразуемого информационного блока другим символом из того же алфавита (соответственно группой символов того же размера и из того же алфавита). Узлы, реализующие эти преобразования, называются, соответственно, P-блоками (P-box, permutation box) и S-блоками (S-box, substitution box).

В 1973-74 гг. Национальное Бюро Стандартов США (NBS) опубликовало документы, содержащие требования к криптографическому алгоритму, который мог бы быть принят в качестве стандарта шифрования данных в государственных и частных учреждениях. В 1976 г. в качестве такового стандарта был утвержден алгоритм, разработанный фирмой IBM. В 1977 г. этот стандарт был официально опубликован и вступил в силу как федеральный стандарт США для шифрования данных - Data Encryption Standard или сокращенно DES [5.2].

В самом схематичном виде DES представляет собой 16-цикловой итерационный блочный шифр. DES работает с блоками данных разрядностью 64 бита с ипользованием 56-разрядного ключа. Применяемые преобразования - поразрядное сложение по модулю два, подстановки и перестановки. Алгоритм выработки 48-битовых цикловых ключей из

56-битового ключа системы и ряд преобразований служат для обеспечения необходимого перемешивания и рассеивания перерабатываемой информации, однако при анализе DES чаще всего играют не самую существенную роль.

В 1999 г. на конференции, организованной RSA, компания Electronic Frontier Foundation взломала ключ DES менее чем за 24 часа. Одной из замен DES, получившей широкое распространение, стал алгоритм Triple DES. В этом случае алгоритм DES выполняется трижды, при этом используются 3 ключа, каждый из которых состоит из 56 битов (что, по сути, соответствует использованию 168-битного ключа). Тем не менее, криптоаналитики обнаружили способ, позволяющий сделать атаку прямого перебора эквивалентной атаке на 108-битовый ключ. Второй проблемой является значительное снижение скорости зашифрования и расшифрования данных.

В ответ на проблемы с длиной ключа и производительностью, проявившиеся в Triple DES, многие криптографы и компании разработали новые блочные шифры. Наиболее популярными предложениями стали алгоритмы RC2 и RC5 [5.3] корпорации RSA Data Security, IDEA [5.5] компании Ascom, Cast [5.4] компании Entrust, Safer [5.6] компании Cylink и Blowfish [5.7] компании Counterpane Systems. Коммерческие альтернативы DES получили определенное распространение, но ни одна из них не стала стандартом.

В 1997 г. Национальный институт стандартов и технологий США (NIST) объявил о начале программы по принятию нового стандарта криптографической защиты. В октябре 2000 г. конкурс завершился. Победителем был признан шифр Rijndael [5.8], разработанный бельгийцами Д. Дейменом и В. Райменом. Алгоритм Rijndael стал основой для нового американского стандарта AES (Advanced Encryption Standard), который в 2001 г. пришел на смену DES и Triple DES и действует и по сей день. Rijndael - это итерационный блочный шифр, имеющий архитектуру "Квадрат". Он быстрый, простой, защищенный, универсальный и хорошо подходит для реализации на смарт-картах. Шифр имеет переменную длин у блоков и различные длины ключей. Длина ключа и длина блока могут быть равны независимо друг от друга 128, 192 или 256 битам. В стандарте AES определена длина блока, равная 128 битам. Шифр AES характеризуется хорошей устойчивостью по отношению к атакам по мощности и по времени. Именно этот шифр рекомендует использовать Microsoft для симметричного шифрования.

Отечественный стандарт шифрования носит официальное название "Алгоритм криптографического преобразования ГОСТ 28147-89" [5.10]. Как явствует из его номера, стандарт был принят в СССР в 1989 г. Если охарактеризовать алгоритм ГОСТ в самом общем виде, то он является блочным шифром, построенным по схеме Фейстеля с 32 циклами шифрования. Длина информационного блока - 64 бита, длина ключа - 256 бит.

Основные отличия алгоритма ГОСТ от алгоритма DES - в строении функции, которая осуществляет отображение $Z_2^{32} \times Z_2^{48} \to Z_2^{32}$, и алгоритме выработки цикловых ключей. И в том и в другом случае преобразования, используемые в алгоритме ГОСТ, проще для программной реализации. Исследования [5.9] показывают, что российский стандарт не уступает по стойкости американскому AES.

Основная идея поточного шифрования состоит в том, что каждый из последовательных знаков открытого текста подвергается своему преобразованию. В идеале разные знаки открытого текста подвергаются разным преобразованиям, т.е. преобразование, которому подвергаются знаки открытого текста, должно изменяться с каждым следующим моментом времени. Реализуется эта идея следующим образом. Некоторым способом получается последовательность знаков $k_1, k_2, \ldots,$ называемая ключевым потоком (keystream) или бегущим ключом (running key, RK). Затем каждый знак x_i открытого текста подвергается обратимому преобразованию, зависящему от k_i - соответствующего знака ключевого потока.

Поточные шифры почти всегда работают быстрее и обычно требуют для своей реализации гораздо меньше программного кода, чем блочные шифры. Наиболее известный поточный шифр был разработан Р. Ривестом; это шифр RC4, который характеризуется переменным размером ключа и байт-ориентированными операциями. На один байт требуется от 8 до 16 действий, программная реализация шифра выполняется очень быстро. Независимые аналитики исследовали шифр, и он считается защищенным. RC4 используется для шифрования файлов в таких изделиях, как RSA SecurPC. Он также применяется для защиты коммуникаций, например, для шифрования потока данных в Интернет-соединениях, использующих протокол SSL.

В число шифров, которые Microsoft по тем или иным причинам не рекомендует использовать для симметричного шифрования, входят следующие:

DES (Причины: малая длина ключей - 56 бит; если в 1993 г. атака на алгоритм заняла 3,5 часа на машине стоимостью $1 млн., то сегодня взлом можно осуществить в реальном времени; 3DES является более защищенным, но наличие лучших вариантов делает его использование неоправданным);

IDEA (International Data Encryption Standard)- хотя длина ключа (128 бит) является приемлемой, Microsoft проводит аналогии с алгоритмом DES: как известно, NSA подозревалось в сознательном ослаблении алгоритма DES, чтобы легко просматривать зашифрованные сообщения;

RC2 и RC5 - причины недоверия Microsoft к этим шифрам те же, что к DES и IDEA. Поскольку для шифрования используются "одноразовые блокноты", слабым местом может стать генератор псевдослучайных последовательностей. Современной тенденцией является использование блочных шифров в режиме поточного шифрования (например, поточное шифрование обеспечивают режимы CBF и OFB для алгоритма DES или режим гаммирования для алгоритма ГОСТ 28147-89);

Blowfish и Twofish - криптоалгоритмы, разработанные Брюсом Шнайером (B. Schneier), удовлетворяют требованиям стойкости, но не являются стандартами: Twofish, являющийся более поздней версией Blowfish, вышел в финал конкурса на замену DES, но уступил шифру Rijndael ;

CAST: несмотря на то, что алгоритм показал себя устойчивым к линейному и дифференциальному криптоанализу, он имеет слишком малую длину ключа - 64 бита;

ГОСТ 28147-89: Microsoft подозревает стойкий шифр в наличии "лазеек" - "backdoors".

Криптоалгоритмы с открытым ключом

В асимметричной криптографии для зашифрования и расшифрования используются различные функции. Стойкость асимметричных криптоалгоритмов базируется на разрешимости лежащих в их основе математических проблем. Пока не найден полиномиальный алгоритм решения этих проблем, данные алгоритмы будут стойки. В этом заключается отличие симметричного и асимметричного шифрования: стойкость первого является непосредственной и научно доказуемой, стойкость второго - предположительной. Кроме того, асимметричные криптоалгоритмы требуют гораздо более интенсивных вычислений и потому являются более медленными.

Наиболее известные криптосистемы с открытым ключом:

Рюкзачная криптосистема (Knapsack Cryptosystem) [5.13];

Криптосистема RSA ;

Криптосистема Эль-Гамаля - EGCS (El Gamal Cryptosystem);

Криптосистема, основанная на свойствах эллиптических кривых - ECCS (Elliptic Curve Cryptosystems).

Применение алгоритмов шифрования с открытым ключом позволяет:

избавиться от необходимости секретных каналов связи для предварительного обмена ключами;

свести проблему взлома шифра к решению трудной математической задачи, т.е., в конечном счете, принципиально по-другому подойти к обоснованию стойкости криптосистемы;

решать средствами криптографии задачи, отличные от шифрования, например, задачу обеспечения юридической значимости электронных документов.

Для решения проблемы, описанной в последнем пункте, были предложены различные схемы электронно-цифровой подписи (ЭЦП). ЭЦП позволяет аутентифицировать автора информации, передающейся в цифровом виде. В определенных ситуациях (например, в электронной коммерции при осуществлении сделок по купле или продаже) ЭЦП по юридической силе приравнивается к обычной подписи "от руки". Кроме того, электронная подпись позволяет убедиться в том, что информация не была искажена при передаче.

Схема ЭЦП должна определять три следующих алгоритма:

алгоритм подписи;

алгоритм проверки подписи.

алгоритм генерации ключевой пары для подписи и ее проверки;

RSA [5.14] - криптографическая система с открытым ключом, обеспечивающая оба механизма защиты: шифрование и цифровую подпись. Криптосистема RSA была разработана в 1977 году и названа в честь авторов: Рональда Ривеста, Ади Шамира и Леонарда Адлемана.

Принцип её действия в следующем. Берутся два больших случайных простых числа p и q приблизительно равной разрядности и вычисляется их произведение $n = pq$. Затем выбирается число e, взаимно простое с произведением $(p-1)(q-1)$ и вычисляется число $d = e^{-1}(mod(p-1)(q-1))$, взаимно простое с n.

Числа e и n становятся открытым ключом, число d - закрытым. Чтобы создать шифртекст c, отправитель возводит сообщение m в степень e по модулю n, где e и n - показатели открытого ключа получателя: $c = m^e(modn)$.

Чтобы расшифровать полученный шифртекст c, получатель вычисляет c в степени d по модулю $n : m = c^d(modn)$.

Если абонент А хочет подтвердить свое авторство сообщения, он сначала шифрует его на своем секретном ключе, а потом на открытом ключе абонента Б. Соответственно, абонент Б применяет к полученному сообщению свой секретный ключ и открытый ключ абонента А; успешное расшифрование является гарантией того, что отправить сообщение мог только абонент А.

Схема Эль-Гамаля [5.15] основана на трудности вычисления дискретных логарифмов в конечном поле в сравнении с лёгкостью возведения в степень в том же самом поле.

Для генерации пары ключей сначала выбирается простое число p и два случайных числа, g и x; оба эти числа должны быть меньше p. Затем вычисляется $y = g^x(modp)$.

Открытым ключом становятся y, g и p. И g, и p можно сделать общими для группы пользователей. Закрытым ключом является x. Теперь, чтобы зашифровать сообщение m, сначала выбирается случайное k, взаимно простое с $p-1$. Затем вычисляются $a = g^k(modp), b = y^k m(modp)$. Пара a и b является шифртекстом, что увеличивает исходное сообщение в два раза. Для расшифрования вычисляется $m = b/a^x(modp)$.

На схеме Эль-Гамаля базировались стандарты ЭЦП в России и США, принятые в 1994 году [5.17, 5.16] и действовавшие вплоть до 2001 г.

Последние математические достижения показали, что проблема логарифмирования в конечных полях не является достаточно прочным фундаментом. Наиболее эффективные на сегодняшний день алгоритмы дискретного логарифмирования имеют уже не экспоненциальную, а субэкспоненциальную временную сложность. Это алгоритмы "index-calculus", использующие факторную базу, к числу которых относятся алгоритм Адлемана [5.18], несколько версий "COS" (алгоритма Копперсмита-Одлыжко-Шреппеля) [5.19] и решето числового поля [5.20]. Ведутся работы по повышению эффективности этих алгоритмов. Так, метод, описанный в [5.21], направлен на повышение эффективности решения линейных уравнений в кольцах вычетов, поскольку все субэкспоненциальные методы дискретного логарифмирования сводятся к этой задаче.

Ряд успешных атак, описанных, например, в [5.23], на системы, основанные на сложности дискретного логарифмирования в конечных полях, привел к тому, в 2001 г. России и США были приняты новые стандарты на ЭЦП [5.22, 5.24]. Процессы формирования и проверки электронной ЭЦП существенно не изменились, однако вместо элементов конечного поля $GF(2^n)$ или $GF(p)$ они оперируют эллиптическими числами, т.е. решениями уравнения эллиптических кривых над указанными конечными полями, а роль операции возведения в степень в конечном поле выполняет операция взятия кратной точки эллиптической кривой. Если старый российский стандарт ЭЦП оперирует 1024-битовыми блоками, то новый - 256-битовыми, но при этом обладает большей стойкостью. Важно отметить, что специальный выбор типа эллиптической кривой позволяет не только во много раз усложнить задачу взлома схемы ЭЦП, но и уменьшить рабочий размер блоков данных. Криптосистемы на основе эллиптической кривой получают все большее распространение скорее как альтернатива, а не замена системам на основе RSA. Они имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Так, согласно стандарту США [5.24] на выработку и верификацию цифровой подписи DSS (Digital Signature Standard), ЭЦП может вырабатываться по одному из трех алгоритмов: DSA (Digital Signature Algorithm), основанному на проблеме дискретного логарифма в конечном поле, ANSI X9.31 (RSA DSA) [5.26] или ANSI X9.63 [5.25] (EC DSA - алгоритм выработки подписи, основанный на проблеме дискретного логарифма в группе точек эллиптической кривой над конечным полем).

Шифрование на платформе Windows

Шифрование - это форма криптографии, предназначенная для преобразования открытого текста с помощью некоторого алгоритма таким образом, чтобы результат был бессмыслицей для лица, не обладающего некоторым секретом для раскрытия исходных данных. Шифрование лежит в основе таких мер безопасности, как цифровая подпись, цифровой сертификат, инфраструктура открытых ключей и др. Перечисленные технологии позволяют повысить безопасность операций, выполняемых с использованием вычислительной техники. Для зашифрования и расшифрования информации используются ключи. Ключ - это переменная, длина которой измеряется в битах. Чем больше двоичных разрядов в используемом ключе, тем сложнее в общем случае будет взломать шифр.

На платформах Windows XP и Windows Server 2003 компания Microsoft рекомендует использовать следующие криптографические алгоритмы [5.11]:

AES-128 (или AES-192, или AES-256);

RSA 2048 (или с еще более длинным ключом);

SHA-2 (т.е. SHA-256 или SHA-512);

DSA (или SHA-2 / RSA).

Криптография Windows Vista (и Longhorn Server) соответствует рекомендациям Агентства Национальной Безопасности США и Национального института стандартов и

технологии (NIST) по реализации протоколов "Suite B" [5.12] и предусматривает использование асимметричных криптоалгоритмов на основе эллиптических кривых. Алгоритмы "Suite B" включают:

AES (шифрование);

EC-DSA (электронно-цифровая подпись);

EC-DH или EC-MQV (обмен секретными ключами);

SHA-2 (хеширование).

Далее мы более подробно рассмотрим алгоритмы шифрования (с секретным и открытым ключом) и алгоритмы хеширования, а также приведем рекомендации Microsoft относительно их применения.

Краткие итоги

В данной лекции рассмотрены основные понятия и определения из области криптографии. Описаны схемы работы симметричных и асимметричных шифров. Указаны стандарты, регламентирующие использование криптографии в России и США. Представлены рекомендации Microsoft по применению криптографических алгоритмов.

5.5 ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ В ИНТЕРНЕТ-БАНКИНГЕ

Интернет-банк – это система удаленного доступа к управлению своими счетами через Интернет на сайте банка. Это виртуальное общение с банком, через сайт в интерактивном режиме. Для работы в ней необходимо подключение этой услуги в офисе банка или по телефону и наличие компьютера с выходом в Интернет. Подключение и обслуживание в этих системах, как правило, бесплатное. Клиент оплачивает только стандартные банковские комиссии за проведение платежей.

В виртуальном офисе банка можно совершать разнообразные операции – список услуг практически тот же, что и в любом реальном отделении. Исключения составляют лишь операции с наличными и операции, связанные с проверкой документов.

В целом подобные системы могут позволять:

проверить состояние счета и получить выписку за любой промежуток времени, делать переводы на счета юридических и физических лиц;

переводить деньги между своими счетами, а также осуществлять перевод между счетами в разной валюте в режиме онлайн;

производить оплату кредита (осуществив перевод с текущего счета), посмотреть список операций по кредитной карте и др.

Есть также ряд специальных услуг – например, срочный депозит. Клиент имеет возможность в режиме онлайн выбрать вид и сумму, валюту депозита, а также счет для зачисления процентов. После этого срочный депозит будет открыт, причем пользователю даже не понадобится ехать в отделение банка.

С помощью интернет-банков можно оплатить:

коммунальные платежи;

услуги операторов связи (мобильный телефон, стационарная связь);

Интернет и коммерческое телевидение;

страховые взносы;

налоги;

штрафы за нарушение ПДД, госпошлины и др.

Для удобства использования и обеспечения оперативного доступа к регулярным платежам возможно создание шаблонов для этих платежей или переводов. Для межбанковских переводов удобна такая подсказка: после ввода БИК (банковского идентификационного кода) банка – получателя платежа все остальные его данные заполняются автоматически. В некоторых системах можно настроить автоматическое проведение регулярных платежей или отложенный платеж, например до поступления средств на счет. Если вы допустили ошибку в реквизитах, вводя данные платежа, то

исправить ошибку и направить зависшие деньги по верному пути можно, только посетив банк.

Все системы интернет-банкинга работают по одинаковому принципу. С клиентом заключается договор, после чего ему дают логин и пароль, с помощью которых можно войти на сайте банка в свой личный кабинет. Там заполняются параметры платежа (ФИО, номер договора на обслуживание, код коммунального платежа и т. п.) и указывается требуемая сумма. Никаких специальных навыков не нужно.

Самые очевидные преимущества – интернет-банкинг позволяет управлять своими счетами из любого места круглосуточно. Кроме этого, большинство операций в Интернете осуществляется мгновенно, и комиссии по многим операциям в интернет-банке ниже, чем при визите в отделение банка.

Безопасность

Эксперты утверждают, что в настоящее время клиенты интернет-банкинга рискуют не больше владельцев карточек, пользующихся банкоматами или терминалами. Прежде чем получить доступ к системе, любой клиент проходит идентификацию (авторизацию) и аутентификацию. Безопасность достигается, как правило, с помощью пароля, контрольного вопроса, электронной подписи (аналог обычной, представляет собой известный только пользователю набор цифр). Существуют также переменные коды и карты доступа, страхующие компьютеры клиентов от вирусов.

Банки настоятельно рекомендуют клиентам просматривать счета и совершать операции только с личного компьютера, поскольку при выходе в Интернет с чужого компьютера возрастают риски утраты конфиденциальной информации.

На сегодняшний день самая распространенная мошенническая схема, приносящая громадные убытки банкам – это фишинг. Фишеры делают массовую рассылку якобы от службы безопасности банков, в которых содержится просьба пройти авторизацию на сайте. Интернет-ресурс, на который ведет ссылка, в точности копирует дизайн сайта банка, а адрес сайта отличается от оригинала на 1-2 символа. Таким образом, конфиденциальная информация попадает к злоумышленникам, а средства исчезают со счетов. Пока что возмещение убытков от деятельности фишеров лежит на банках.

Мобильный банкинг

Мобильный банкинг – управление банковским счетом с помощью планшетного компьютера, смартфона или обычного телефона. Как правило, для этого на мобильное устройство необходимо загрузить специальное мобильное приложение.

В большинстве случаев для совершения банковских операций требуется доступ в Интернет. Реже транзакции осуществляются с помощью отправки СМС-сообщений. Можно отметить, что ранее, до того как смартфоны получили широкое распространение, именно СМС-банкинг считался мобильным банкингом.

В настоящее время приложения для мобильного банкинга – это приложения для интернет-банкинга с урезанным функционалом, адаптированные под небольшие экраны смартфонов и под операционные системы, устанавливаемые в мобильных устройствах. В будущем мобильный банкинг обещает быть, напротив, более функциональным, чем обычный интернет-банкинг, поскольку мобильные устройства позволяют с удобством для клиента использовать технологии голосовой идентификации, создавать шаблоны платежей с помощью встроенной в телефон камеры и т. д.

Одну из самых продвинутых систем мобильного банкинга разрабатывает Сбербанк России, который заявил о том, что готовит приложения для 30 тыс. мобильных устройств с учетом всех технологических особенностей телефонов и смартфонов – наличия функциональных кнопок, размера экрана и т. д.

На сегодняшний день банки выпускают приложения для мобильного банкинга, ориентированные на мобильные устройства, работающие под управлением операционных систем iOS и Андроид.

Меры безопасности при использовании мобильного банка:

При потере мобильного телефона Вам следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка для блокировки услуги «Мобильный банк».

При смене номера телефона, на который подключена услуга «Мобильный банк», Вам необходимо отключить услугу «Мобильный банк» от старого номера телефона и подключить услугу на новый номер. Помните, что операторы сотовой связи могут передать номер телефона другому абоненту, если он будет неактивным длительное время.

Будьте внимательны – не оставляйте свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг. Установите на телефоне пароль, данная возможность доступна для любых современных моделей телефонов/смартфонов.

Не подключайте к услуге «Мобильный банк» телефоны, которые вам не принадлежат, по просьбе третьих лиц, даже если к вам обратились от имени сотрудников банка.

При установке на телефон дополнительных программ обращайте внимание на полномочия, которые необходимы программе. Если программе требуются излишние полномочия это повод проявить настороженность (доступ и отправка SMS, доступ к Интернет и др.).

Установите на телефон антивирусное ПО и своевременно его обновляйте. Для платформы Андроид рекомендуем бесплатные приложения DrWeb for Андроид Light и Kaspersky Internet Security for Андроид (доступно для загрузки из Google Play).

При внезапном прекращении работы SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин – в отношении вас возможно проведение мошеннических действий третьими лицами.

Не взламывайте телефон (например, через Jailbreaking), так как это отключает защитные механизмы, заложенные производителем. В результате ваш телефон становится уязвимым к заражению вирусным ПО.

Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по SMS/электронной почте, в том числе от имени банка.

Отключайте в настройках вашего iPhone возможность использовать голосовое управление Siri на заблокированном экране.

При подозрении, что от вашего имени осуществляются несанкционированные вами операции, банк по своей инициативе может временно заблокировать услугу «Мобильный Банк». Для возобновления потребуется связаться с банком и подтвердить легитимность подключения и сделанных операций.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

6.1.1. Перечень основной литературы

1. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html.

2. Макаров А.М. Организация защиты персональных данных [Электронный ресурс] : лабораторный практикум / А.М. Макаров, И.В. Калиберда, К.О. Бондаренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 92 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62971.html.

6.1.2. Перечень дополнительной литературы

1. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52153.html.

2. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [Электронный ресурс] / А.И. Савельев. — Электрон. текстовые данные. — М. : Статут, 2017. — 320 c. — 978-5-8354-1365-2. — Режим доступа: http://www.iprbookshop.ru/65895.html.

6.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению практических занятий по дисциплине по дисциплине «Персональная кибербезопасность».

2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Персональная кибербезопасность».

6.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Университетская библиотека online. http://www.biblioclub.ru;
2. ЭБС «IPRbooks». http://www.iprbookshop.ru;
3. Электронная библиотека СКФУ.а. http://catalog.ncstu.ru;
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.