ОЦЕНКА РИСКОВ ХИЩЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ГОМОМОРФНОГО ШИФРОВАНИЯ

А. И. ТРУБЕЙ, В. Б. АЛЮШКЕВИЧ, Т. С. МАРТИНОВИЧ, Д. С. КИМ

Оценим некоторые наиболее типичные риски утечки конфиденциальной информации с использованием методик GlobalTrust и Системы оценки общеизвестных уязвимостей (Common Vulnerability Scoring System – CVSS).

Методика GlobalTrust соответствует требованиям стандартов СТБ ISO/IEC 27001, СТБ ISO/IEC 27005, ISO/IEC 27035 и базируется на известных методах оценки рисков CRAMM, OCTAVE и RA2. Величина риска, соответствующая прогнозируемым среднегодовым потерям, ALE (Annual Loss Expectancy) рассчитывается по формуле

$$ALE = AV \cdot EF \cdot ARO, \quad (1)$$

где AV (Asset Value) – стоимость актива; EF(Exposure Factor) – степень уязвимости актива к угрозе; ARO (Annualized Rate of Occurrence) – среднегодовая частота возникновения инцидентов, величина, представляющая собой ожидаемую частоту реализации угрозы в год.

Система CVSS состоит из 3 групп метрик: базовые, временные и контекстные метрики. Каждая метрика представляет собой число в интервале 0 – 10 и вектор – краткое описание со значениями, используемыми для вывода оценки. Базовые метрики используются для описания основополагающих сведений об уязвимости. Метрики: вектор доступа (AV), сложность доступа (AC) и аутентификация (Au) оценивают возможность получения доступа к уязвимости и необходимость для эксплуатации уязвимости дополнительных условий. Метрики воздействия: влияние на конфиденциальность (C), целостность (I) и доступность (A) описывают разрушительность атаки в случае эксплуатации уязвимости. Временные метрики отражают характеристики уязвимостей, изменяющихся во времени. К ним относятся временные метрики: воздействие на возможность эксплуатации **(**E), уровень устранения (RL), степень достоверности информации (RC). Контекстные метрики позволяют адаптировать оценку к конкретной ИС. К ним относятся: возможность сопутствующего ущерба (CDP), распределение целей (TD), требования к конфиденциальности (CR), целостности (IR), доступности (AR).

На первом этапе проводится расчет оценки для базовых метрик, на которую затем накладываются временные и контекстные оценки. В дальнейшем будем использовать только базовые и временные метрики для вычисления оценки по формуле

$$TS=[((0{,}6\cdot 10{,}41\cdot(1-(1-C)\cdot(1-I)\cdot(1-A))+(0{,}4\cdot 20\cdot AV\cdot AC\cdot Au)-1{,}5)\cdot 1{,}176]\cdot E\cdot RL\cdot RC. \quad (2)$$

Оценки уязвимостей пронормируем (EF=CVSS Raiting/10) для получения значений в интервале (0;1), что позволит использовать их при расчете рисков по формуле (1):

Вероятность использования уязвимости вычислим с применением базовых метрик возможности эксплуатации и временных метрик по формуле

$$P_E = AV\cdot AC\cdot Au\cdot E\cdot RL\cdot RC. \quad (3)$$

1. Оценка риска хищения конфиденциальной информации пользователем локальной сети, реализующей обработку геолого-геофизических данных (Скиф-недра).

Будем рассматривать ИС, реализующую высокопроизводительные информационно-вычислительные технологии обработки геолого-геофизических данных. Оценим риск хищения конфиденциальной информации, к которой не был предусмотрен до-

ступ по политике безопасности, злоумышленником из числа пользователей ИС с использованием привилегий. Для оценки риска будем использовать откалиброванную качественную шкалу, приведенную в таблице 1. В основу оценки ущерба положим подход, применяемый в УК Республики Беларусь (глава 24), в предположении, что стоимость *ИС* совместно с активами и оказываемыми услугами составляет Са млн руб.

Таблица 1

Качественная шкала оценки ущерба согласно УК РБ

Уровень ущерба (риска)	**Среднегодовой ущерб в результате инцидентов безопасности – ALE (млн руб.)**
Незначительный	0 ≤ ALE < 40 базовых величин
Значительный	40 базовых величин ≤ ALE < 250 базовых величин
Крупный	250 базовых величин ≤ ALE < 1000 базовых величин
Особо крупный	1000 базовых величин ≤ ALE < 0,5·Са
Неприемлемый	0,5·Са ≤ ALE

В качестве информационных активов возьмем геологические, геофизические и иные данные, характеризующие особенности строения и минерально-сырьевой потенциал недр, зафиксированные на материальных носителях, накопленные и обрабатываемые в ИС. Хищение данных приведет к нарушению их конфиденциальности и прав собственности. Возможно, придется уплачивать штрафы по искам клиентов.

Вероятность уязвимости оценим по методике CVSS. Для уязвимости, имеющей несколько способов эксплуатации, будем выбирать метод, оказывающий наибольшее воздействие. В метрике Au для локально эксплуатируемых уязвимостей значения S или M присваиваем, если необходима дополнительная аутентификация, кроме той, которая требуется при регистрации в системе. Уязвимости, предоставляющие доступ с пользовательским уровнем привилегий, оцениваются как частичная потеря конфиденциальности, целостности и доступности.

Значения базовых метрик: AV – локальный (L = 0,395); AC – высокая (H = 0,35); Au – многократная (M = 0,45); C – частичное (P = 0,275); I – частичное (P = 0,275); A – частичное (P = 0,275). Получим базовый вектор: AV: L / AC: H / Au: M / C: P / I: P / A: P. Значения временных метрик: E – функциональное (F = 0,95); RL – временное решение (TF = 0,90); RC – не подтверждена (UC=0,90). Получим временной вектор: E: F / RL: TF / RC: UC.

По формуле (2) вычислим TS = 2,6 (после нормирования EF = 0,26). Согласно шкале FortiGuard, приведенной в таблице 2, уровень опасности данной уязвимости – «низкий».

Таблица 2

Шкала опасности уязвимостей FortiGuard

Уровень опасности FortiGuard	**Оценка по CVSS 2.0**
Критический	9 – 10
Высокий	7 – 8,9
Средний	4 – 6,9
Низкий	0,1 – 3,9
Информационный	0

По формуле (3) получим: P_E = L·H·M·F·TF·UC = 0,395·0,35·0,45·0,95·0,9·0,9 = 0,05.

В предположении, что пользователь еженедельно имел возможность осуществлять несанкционированный доступ с использованием привилегий, получим ARO = 52·0,05 = 2,6.

Если Ca = 10 млрд руб., AV=100 млн руб., то ALE = 100·0,26·2,6 = 70 млн руб. Согласно таблице 1 это «крупный» уровень ущерба.

2. Оценка риска хищения геолого-геофизических данных, обрабатываемых в публичной облачной системе.

Оценим риск хищения вышеописанной конфиденциальной информации при ее обработке в публичной облачной системе. Следует учитывать, что клиенты IaaS обеспечивают управление доступом к ОС, бизнес-приложениям и ПО, безопасность конфигурации приложений и ПО, антивирусную защиту. Уязвимости, при которых обеспечивается доступ на корневом уровне, будем оценивать как полную потерю конфиденциальности, целостности и доступности. Получим следующие результаты.

Значения базовых метрик: AV – сетевой (N = 1,0); AC – низкая (L = 0,71); Au – однократная (S = 0,56); C – полное (C = 0,66); I – полное (C = 0,66); A – полное (C = 0,66). Получим базовый вектор: AV: N / AC: L / Au: S / C: C / I: C / A: C. Значения временных метрик: E – высокое (H = 1,0); RL – официальное исправление (OF = 0,87); RC – подтверждена (C=1,0). Получим временной вектор: E: H / RL: OF / RC: C.

По формуле (2) вычислим TS = 7,8 (после нормирования EF = 0,78), что согласно таблице 2 соответствует уровню опасности – «высокий».

По формуле (3) получим: P_E = N·L·S·H·OF·C = 1·0,71·0,56·1·0,87·1 = 0,35, ARO = 18,2.

ALE = 100·0,78·18,2 = 1400 млн руб. Это «особо крупный» уровень ущерба.

То есть, риск хищения информации в публичном облаке примерно в 20 раз выше, чем в локальной сети. Поэтому необходимо применять дополнительные средства защиты, например, гомоморфного шифрования, при ее обработке в публичном облаке.

3. Области применения гомоморфного шифрования.

Гомоморфное шифрование является формой шифрования, позволяющей выполнить определенную алгебраическую операцию над открытым текстом посредством выполнения (возможно, другой) алгебраической операции над зашифрованным текстом.

Система шифрования является гомоморфной относительно операции: умножения, если $D(E(m_1)\otimes E(m_2)) = m_1 \times m_2$; сложения, если $D(E(m_1)\oplus E(m_2)) = m_1+m_2$. Система шифрования является полностью гомоморфной, если справедливы оба утверждения, то есть $D(E(m_1)\otimes E(m_2)) = m_1 \times m_2$ и $D(E(m_1)\oplus E(m_2)) = m_1+m_2$, где $\otimes$, $\oplus$ – операции умножения и сложения над шифрованными текстами, соответствующие операциям ×, + над открытыми текстами, D – функция расшифрования, E – функция шифрования.

3.1. ***Облачные вычисления.*** В облачных вычислениях следует применять алгоритмы, которые лучше всего справляется с поставленной задачей. Для умножения зашифрованных данных можно использовать алгоритмы RSA или Эль-Гамаля, а для сложения — Пэйе. Возможно использование комбинированных систем данных алгоритмов. Предпочтительным является использование гомоморфного шифрования в гибридных облачных системах, так как вычисления, которые не могут быть вынесены в публичное облако в силу законодательных или иных ограничений, могут производиться во внутренней сети.

3.2. ***Электронное голосование.*** С помощью гомоморфной системы можно зашифровать голоса избирателей и провести расчеты над зашифрованными данными, сохраняя анонимность избирателей. В качестве системы шифрования при тайном голосовании, включая тайное голосование с весами, можно использовать систему Пэйе.

3.3. ***Защищенный поиск информации.*** Гомоморфное шифрование может предоставить пользователям возможность извлечения информации из поисковых систем с сохранением конфиденциальности – сервисы смогут получать и обрабатывать запросы, а также выдавать результаты обработки, не анализируя и не фиксируя их реальное содержание.

3.4. ***Защита беспроводных децентрализованных самоорганизующихся сетей (MANET).*** Для обеспечения безопасности данных в сетях MANET может применяться гомоморфное шифрование, которое может быть встроено в протоколы маршрутизации.

3.5. ***Системы с обратной связью (secure feedback system).*** Используются для обеспечения анонимности пользователей и скрытия промежуточных результатов вычислений. Они осуществляют сбор отзывов о работе студентов/преподавателей. Полученные отзывы гомоморфно шифруются и сохраняются для последующих вычислений.

3.6. ***Обфускация для защиты программных продуктов.*** Впервые о применении обфускации в криптографии было упомянуто в работе Диффи и Хеллмана. В ней предложено использовать для построения асимметричной криптосистемы сложность задачи, заключающейся в анализе программ на низкоуровневом языке программирования. Поскольку все традиционные компьютерные архитектуры используют двоичные строки, поэтому с применением полностью гомоморфного шифрования над битами можно вычислить любую функцию. Следовательно, можно гомоморфно зашифровать всю программу так, что она сохранит свою функциональность.

3.7. ***Аутсорсинговые услуги для смарт-карт.*** Особо ресурсоемкие приложения могут работать вне карты на гомоморфно зашифрованных данных. Они могут воспользоваться более мощными внешними устройствами хранения и процессорами, например, для проведения биометрических проверок (распознавание голоса, отпечатков пальцев, почерка).

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ МАССОВОЙ ИНФОРМАТИЗАЦИИ ОБЩЕСТВА

Е. А. СВИРСКИЙ

В настоящее время происходит быстрое обновление прикладных знаний, что приводит к такому же быстрому появлению новых технологий. Особенно это касается информационных технологий. Современные ИТ-технологии открывают широчайшие возможности для общения и достижения результатов в самых различных областях. Особенно стремительно развиваются мобильные ИТ-технологии, которыми уже пользуются различные слои населения. На них возлагаются большие надежды в смысле объединения в одном устройстве широкого спектра услуг. Это очень удобно для пользователей, быстрый доступ к телефонной связи, интернету, к мобильным банковским услугам и т. д. Очевидная выгода есть и для поставщиков услуг – наличие обширной сети пользователей мобильных ИТ-технологий позволяет наращивать мобильные услуги. В этом секторе деятельности общества достигнут существенный прогресс. Но у этого прогресса есть и вторая сторона, которая подавляющим числом пользователей ИТ-технологий недооцениваться, а чаще всего и вообще не воспринимается, а, как известно, достижениями прогресса можно воспользоваться и не в столь благовидных целях. Не задумываясь о вопросах безопасного использования ИТ-технологий, их пользователи подвергают риску себя, свою работу, свою семью.

Эволюция технического обеспечения, которое включает в себя аппаратные средства, средства коммуникации, программное обеспечение, протекает неравномерно, скачкообразно. Развитие компьютерной техники происходит в геометрической прогрессии. Каждые полтора года производительность компьютеров увеличивается в 2 раза. Одновременно с ростом производительности компьютеров появляются и новые программные продукты, которые зачастую имеют уязвимости различной степени доступности, выявление которых возможно на всех последующих этапах жизненного цикла программного продукта. Наличие уязвимостей создает для пользователей проблемы с обеспечением защиты информационных ресурсов.

В целом сегодня ИТ-технологии представляют новое оружие конкуренции в различных сферах деятельности, вызывая острую борьбу между фирмами. Так, «Intel» предсказывает, что «электронная» коммерция в конце концов вытеснит среднее звено