ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056:005.342 (083.74)(476)

А.И. Трубей

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СУЩЕСТВУЮЩЕЙ НОРМАТИВНО-ПРАВОВОЙ И МЕТОДИЧЕСКОЙ БАЗЫ

Проводятся обзор и анализ существующей нормативной базы в области менеджмента рисков информационной безопасности, а также теоретических основ и методов их оценки. Предлагаются практические методы оценки рисков и уязвимостей информационной безопасности.

Введение

В настоящее время все больше конфиденциальной информации хранится и обрабатывается в различных информационных системах (ИС). Практически любой ИС присущи уязвимости, обусловливающие возможность реализации угроз обрабатываемой в ней информации. Наиболее вероятными источниками возникновения угроз для защищаемых активов являются обслуживающий персонал, средства вычислительной техники, системное и прикладное программное обеспечение. В этих условиях особое внимание следует уделять анализу и оценке рисков информационной безопасности (ИБ) как необходимым составляющим комплексного подхода к обеспечению ИБ. Решение задачи оценки угроз безопасности для различных ИС является основой для применения необходимых методов и средств защиты информации. Адекватная оценка рисков ИБ позволит осуществлять прогнозирование возможного ущерба, связанного с реализацией угроз, а соответственно, и оценку необходимого размера инвестиций на построение систем защиты информации.

В статье основное внимание уделяется теоретическим и практическим вопросам оценки уязвимостей информации как одной из составных частей оценки риска. Приводятся оценки риска утечки конфиденциальной информации по техническим (радио-) каналам при соблюдении либо несоблюдении соответствующих мер защиты, а также оценки риска хищения конфиденциальной информации, к которой не был предусмотрен доступ по политике безопасности, для локальной сети и (для сравнения) облачной системы.

1. Нормативная база в области менеджмента рисков

Достижение требуемого уровня ИБ в любой организации должно базироваться на исследовании источников угроз информации, уязвимостей в ее защите и обусловленных их соотношением рисков. Механизм эффективного противодействия угрозам ИБ содержится в доступных международных стандартах, прежде всего в современных риск-ориентированных стандартах ISO (International Organization for Standardization) и аналогичных национальных стандартах.

Оценка рисков ИБ и их периодическая переоценка являются неотъемлемой частью создания и функционирования системы менеджмента информационной безопасности (СМИБ), разрабатываемой с целью выбора соразмерных средств управления безопасностью, которые предназначены для защиты информационных активов и придают уверенность заинтересованным сторонам. Данное положение закреплено в СТБ ISO/IEC 27001–2011 [1] (самом популярном в Беларуси стандарте в области ИБ [2]) и других нормативных документах. В частности, в соответствии с приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3 «в целях реализации политики информационной безопасности разрабатываются локальные нормативные правовые акты организации, регламентирующие порядок … выявления угроз, которые могут привести к сбоям, нарушению функционирования ин-

формационной системы» [3]. Это является составной частью мониторинга и анализа СМИБ, а также оценки рисков.

Вследствие большого количества стандартов и подходов к анализу рисков ИБ основные понятия в этой области имеют множество определений. Наиболее подходящим для большинства практических применений является определение риска ИБ, приведенное в СТБ ISO/IEC 27005–2012 [4]. Стандарт основан на общих концепциях, изложенных в [1], и предназначен для содействия адекватному обеспечению ИБ на основе риск-ориентированного подхода. Согласно [4] риск информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации. В стандарте [4] конкретизировано понятие риска ИБ (активы, угрозы, уязвимости и ущерб), рассмотрен процесс менеджмента рисков ИБ, включающий идентификацию, анализ, оценку, обработку и т. д., и предложены две критические точки принятия решения (обрабатывать ли конкретный риск и считается ли данный риск приемлемым). Из стандарта исключено детальное описание рекомендуемого подхода к оценке рисков. Организация может самостоятельно выбирать подходящую методологию.

Негативные последствия широкого круга угроз ИБ (начиная от атак хакеров и заканчивая действиями инсайдеров, применяющих свои знания и права доступа к данным для собственной выгоды) можно уменьшить, используя подход к управлению инцидентами ИБ, описанный в новом стандарте ISO/IEC 27035:2011 [5]. Интеграция системы управления инцидентами ИБ позволит уменьшить негативные последствия от реализации угроз ИБ, повысить общий уровень ИБ, качество оценки и управления рисками ИБ. Стандарт согласован с общими принципами, установленными в [1], и может применяться в любой организации независимо от ее размера.

Заслуживает также упоминания американский стандарт в области менеджмента рисков NIST 800–37:2010 [6], в котором представлен трехуровневый подход к оценке риска. Выделяют уровень ИС, уровень бизнес-процессов и уровень организации. На уровне ИС идентифицируются информационные активы, уязвимости и угрозы, а также применяемые средства защиты.

2. Теоретические основы оценки рисков информационной безопасности

Оценка риска заключается в определении его уровня (качественной либо количественной величины) и сравнении этого уровня с максимально допустимым (приемлемым) уровнем, а также с уровнем других рисков. Другими словами, оценка риска нарушения ИБ – это систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющий провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов на всех стадиях их жизненного цикла.

Уровень риска определяется путем комбинирования двух величин: вероятности инцидента в области ИБ и размеров его последствий. Инцидент заключается в реализации угрозы, использующей уязвимости актива для воздействия на этот актив и нарушения его безопасности. Под безопасностью информационного актива понимаются такие свойства информации, как конфиденциальность (защита от несанкционированного ознакомления), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения) и доступность (возможность за приемлемое время получить требуемую информационную услугу). Иногда к ИБ относят также аутентичность (возможность подтверждения подлинности и достоверности документов) и неотказуемость (невозможность отрицания совершенных действий применительно к информационным активам).

Точно определить вероятности угрозы и уязвимости либо размер ущерба на практике обычно не представляется возможным, поэтому речь может идти только о численных оценках в некотором диапазоне величин. Количественная оценка риска необходима для определения конкретной величины риска, а качественная – для интерпретации полученного результата. Количественную величину риска, связанного с осуществлением конкретной угрозы безопасности в отношении конкретного актива, можно выразить следующим образом:

$$R = P_V \cdot P_T \cdot D, \tag{1}$$

где P_V (вероятность уязвимости) – вероятность успешного использования уязвимости потенциальной угрозой;

P_T (вероятность угрозы) – вероятность того, что угроза в отношении актива будет реализовываться; успех либо неуспех реализации угрозы определяется величиной уязвимости. Анализ методик менеджмента рисков показывает, что в них используется не вероятность реализации угрозы, а примерная частота реализации угрозы за определенный промежуток времени. Для исключения путаницы в стандартах вместо термина probability используется likelihood;

D – величина потенциального ущерба, который может быть причинен при реализации угрозы.

2.1. Вероятность уязвимости

При решении практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. Известно, что несанкционированное получение информации возможно не только путем доступа к базам данных, но и многими другими способами, не требующими такого доступа. Основную опасность представляют преднамеренные действия злоумышленников. Воздействие случайных факторов само по себе не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов утечки информации, которыми может воспользоваться злоумышленник. Потенциально возможные несанкционированные действия могут иметь место во внешней неконтролируемой зоне, зоне контролируемой территории, зоне помещений, зоне активов, зоне баз данных.

При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий:

– нарушитель получил доступ в соответствующую зону;

– во время нахождения нарушителя в зоне проявляется канал утечки;

– канал утечки доступен нарушителю соответствующей категории;

– в канале утечки есть конфиденциальная информация.

По уровню возможностей нарушители могут подразделяться на следующие категории:

Первая категория – пользователи с низким уровнем возможностей, осуществляющие запуск задач (программ) из фиксированного набора, которые реализуют типовые функции по обработке информации.

Вторая категория – разработчики из числа обслуживающего персонала со средним уровнем возможностей, осуществляющие создание и запуск собственных программ с новыми функциями.

Третья категория – администраторы ИС, сотрудники подразделения технической защиты информации с высоким уровнем воздействия на базовое ПО и конфигурацию оборудования.

Четвертая категория – персонал сторонних организаций или самой организации, осуществляющий проектирование и техническое обслуживание ИС с максимальными возможностями: включение в состав ИС аппаратно-программных средств с новыми функциями.

Вероятность уязвимости – несанкционированного получения информации нарушителем *k*-й категории по *j*-му каналу утечки информации в *l*-й зоне *i*-го структурного компонента объекта либо системы – находится по формуле [7]

$$P_{ijkl} = P^{\partial}_{ikl} \cdot P^{к}_{ijl} \cdot P^{и}_{ijkl} \cdot P^{и}_{ijl}, \qquad (2)$$

где P^{∂}_{ikl} – вероятность доступа нарушителя *k*-й категории в *l*-ю зону *i*-го компонента объекта либо системы;

$P^{к}_{ijl}$ – вероятность наличия (проявления) *j*-го канала утечки информации в *l*-й зоне *i*-го компонента объекта либо системы;

$P^{и}_{ijkl}$ – вероятность доступа нарушителя *k*-й категории к *j*-му каналу утечки информации в *l*-й зоне *i*-го компонента при условии доступа нарушителя в зону;

P_{ijl}^{u} – вероятность наличия защищаемой информации в *j*-м канале утечки информации в *l*-й зоне *i*-го компонента.

Вероятность уязвимости принимает значения в диапазоне (0, 1).

2.2. Частота реализации угрозы

Частота реализации угрозы определяется путем экспертных оценок, прогнозирования, а также на основании статистических данных. Является положительным числом, определяющим ожидаемое количество попыток реализации угрозы за определенный период времени.

2.3. Величина ущерба

Величина прямого или косвенного ущерба, причиняемого организации в результате инцидентов безопасности, связанных с раскрытием, несанкционированной модификацией, временной недоступностью или разрушением информации, определяется ценностью информационных активов. Последствия таких инцидентов могут выражаться в упущенной выгоде, потере конкурентных преимуществ, ухудшении имиджа организации, причинении вреда интересам третьей стороны, штрафах, прямых финансовых убытках или дезорганизации деятельности. При этом для каждого актива следует рассматривать наихудший сценарий развития событий.

Оценка ущерба – достаточно сложная задача, плохо поддающаяся формализации и решаемая, как правило, с использованием методов экспертных оценок. Для оценки возможного ущерба могут применяться различные критерии и качественные шкалы. Для того чтобы оценка ущерба имела экономический смысл, качественная шкала должна соотноситься с размером финансовых потерь. Размер ущерба, как правило, выражается в денежных единицах.

3. Краткий обзор методик оценки рисков и уязвимостей

Согласно [1] оценка рисков ИБ необходима для понимания требований ИБ и рисков для активов организации. Наиболее простую и понятную методику управления информационными рисками предлагает группа компаний GlobalTrust, специализирующихся на создании систем защиты информации и персональных данных, а также систем менеджмента информационной безопасности. Методика полностью соответствует требованиям международных стандартов [1–5], представляющих собой практическое руководство по управлению рисками, и базируется на популярных методах оценки рисков, таких как CRAMM, OCTAVE и RA2 [8].

Новая версия методики управления рисками GlobalTrust включает полный комплект документов, необходимых для внедрения системы управления рисками ИБ в организациях любого типа и размера. Методика оценки рисков GlobalTrust характеризуется следующими особенностями:

– риск оценивается для конкретных активов или групп активов;

– риск определяется качественно и количественно на основании трех параметров: вероятности угрозы, величины уязвимости, размера ущерба;

– формируется реестр информационных активов, определяющих для каждого информационного актива его местоположение, формат, принадлежность к классам и категориям пользователей и владельцев, приложения и бизнес-процессы, в которых он используется, а также свойства актива и требования по его доступности;

– для оценки риска используется многоуровневая качественная шкала, дополнительно риски делятся на высокие, средние, низкие; для сопоставления качественных уровней рисков и количественных значений величины риска используется процедура калибровки шкалы оценки риска;

– методика охватывает также процессы обработки риска, предусматривается формирование плана обработки рисков.

Для вычисления рисков удобно использовать период времени, равный одному году. В этом случае величина риска соответствует прогнозируемым среднегодовым потерям организации в результате инцидентов безопасности ALE (Annual Loss Expectancy). Эту величину целесообразно использовать для соотнесения расходов на безопасность с величиной риска.

Величина ALE рассчитывается по формуле

$$ALE = SLE \cdot ARO. \quad (3)$$

Здесь SLE (Single Loss Expectance) – потенциальный ущерб (в денежных единицах) для организации в результате единичного факта реализации соответствующей угрозы:

$$SLE = AV \cdot EF, \quad (4)$$

где AV (Asset Value) – стоимость актива (данных, программ, аппаратуры и т. д.);

EF (Exposure Factor) – степень уязвимости актива к угрозе;

ARO (Annualized Rate of Occurrence) – среднегодовая частота возникновения инцидентов (ожидаемая частота реализации угрозы в год). Значение ARO зависит от эффективности элементов системы защиты и вероятности того, что они не выполнят своих функций.

Таким образом,

$$ALE = SLE \cdot ARO = AV \cdot EF \cdot ARO. \quad (5)$$

Для определения EF используются оценочные количественные значения, полученные путем экспертных оценок, прогнозирования, а также на основании статистических данных из общедоступных источников, например на основании систем оценки уязвимостей, которые созданы коммерческими и некоммерческими организациями. На данный момент существует ряд организаций, занимающихся мониторингом, классификацией и накоплением данных об уязвимостях, которые предоставляют открытый доступ к своим базам уязвимостей. Перечни уязвимостей в этих системах используются как один из основных источников информации для оценки ИБ, так как описания уязвимостей содержат и предусловия, и оценки, характеризующие результат атак, эксплуатирующих эти уязвимости, а также списки конкретных программно-аппаратных средств, содержащих уязвимости.

Каждая из этих систем имеет свои преимущества, но все они отличаются по измеряемому признаку. Например, CERT/CC использует значения оценок от 0 до 180 и учитывает следующие факторы: подвержена ли интернет-инфраструктура риску и какой тип предусловий нужен для эксплуатации уязвимости. При оценке уязвимости по методике SANS кроме простоты эксплуатации учитывается и распространенность уязвимых систем. Компания Microsoft использует методику оценки уязвимостей, связанных с вредоносным программным обеспечением, которая учитывает наличие обновления и количество векторов, применяемых атакующим. В системе DREAD используются минимальное число показателей и очень простая формула для получения общего показателя (простое их усреднение).

По мнению экспертов, одной из наиболее распространенных, востребованных и проверенных на практике является система оценки общеизвестных уязвимостей (Common Vulnerability Scoring System, CVSS) [9, 10]. CVSS предназначена для оценки уязвимостей, связанных с дефектами и ошибками ПО при проектировании или кодировании. Она состоит из трех базовых, временных и контекстных метрик. Каждая метрика представляет собой число (оценку) в интервале 0–10 и вектор – краткое текстовое описание со значениями, которые применяются для вывода оценки.

Базовые метрики (Base Metrics) используются для описания основополагающих сведений об уязвимости (возможности эксплуатации уязвимости и влиянии уязвимости на систему). Их значения практически не меняются со временем и не зависят от окружения, в котором работает оцениваемый продукт. 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. Это влияние определяется независимо относительно конфиденциальности, целостности и доступности.

Временные метрики (Temporal Metrics) отражают характеристики уязвимостей, которые изменяются во времени. К ним относятся метрики «воздействие на возможность эксплуатации **(***E*)», «уровень устранения (*RL*)», «степень достоверности информации (*RC*)».

Группа контекстных метрик (Environmental Metrics) позволяет адаптировать оценку уязвимости к конкретной ИС. Контекстные метрики учитывают конкретное окружение, в котором работает программа. К ним относятся возможность сопутствующего ущерба (*CDP*), распределение целей (*TD*), требования к конфиденциальности (*CR*), целостности (*IR*), доступности (*AR*).

Как правило, базовые и временные метрики определяются аналитиками, разработчиками продуктов в области безопасности или разработчиками приложений, потому что они лучше осведомлены о характеристиках уязвимости, чем пользователи. Контекстные метрики определяются пользователями, поскольку они точнее могут оценить потенциальное воздействие уязвимости в рамках своей собственной среды. 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

$$TemporalScore = TS = [((0,6 \cdot Impact) + (0,4 \cdot Exploitability) - 1,5) \cdot f(Impact)] \cdot E \cdot RL \cdot RC, \qquad (6)$$

где $Impact = 10,41 \cdot (1 - (1 - C) \cdot (1 - I) \cdot (1 - A))$;

$Exploitability = 20 \cdot AV \cdot AC \cdot Au$;

$f(Impact) = 0$, если $Impact = 0$; $f(Impact) = 1,176$ в противном случае.

Оценки уязвимостей по методике CVSS необходимо пронормировать для получения значений в интервале (0;1), что позволит использовать их при расчете рисков по формуле (5):

$$EF = CVSS\ Rating / 10. \qquad (7)$$

Вместо частоты реализации угрозы *ARO* будем определять вероятность эксплуатации уязвимости, которая учитывает как вероятность наличия уязвимости, так и вероятность ее использования хотя бы одной из угроз. Чем выше уровень подверженности уязвимости применению эксплойта, тем больше шансов провести успешную атаку и тем выше частота злонамеренного использования. Вычислим вероятность использования уязвимости с применением базовых метрик возможности эксплуатации и временных метрик по формуле [11]

$$P_E = AV \cdot AC \cdot Au \cdot E \cdot RL \cdot RC. \qquad (8)$$

Частоту реализации угрозы *ARO* будем определять с помощью данной вероятности в каждом конкретном случае оценки риска.

Некоторые наиболее типичные риски утечки конфиденциальной информации можно оценить с помощью методик GlobalTrust и CVSS.

При расчете вероятностей уязвимостей и угроз, а также при оценке рисков осуществляется округление результатов вычислений.

4. Оценка риска утечки информации по радиоканалу

Оценим риск утечки конфиденциальной информации, обрабатываемой в ИС, которая реализует высокопроизводительные информационно-вычислительные технологии обработки геолого-геофизических данных, по радиоканалу (посредством радиоизлучений от внедренных электронных устройств перехвата информации, модулированных информативным сигналом).

Предположим, что технические средства ИС расположены на одном объекте в пределах одной контролируемой зоны и обработка конфиденциальной информации осуществляется в рабочие дни в рабочее время в течение 2 ч. Нарушителя можно отнести к четвертой категории.

Для оценки риска будем использовать следующую качественную шкалу, в которой определенным уровням риска сопоставляются соответствующие размеры среднегодовых потерь. Предположим, что стоимость ИС совместно с активами и оказываемыми услугами составляет Ca млн руб. Поэтому максимальный риск, равный восьми, сопоставим с потерей функциональности всей ИС или ее большей части (банкротством). Минимальный уровень риска, равный нулю, соответствует отсутствию среднегодовых потерь в результате инцидентов безопасности либо минимальным потерям, не превышающим, например, $0{,}0001 \cdot Ca$ млн руб. в год (табл. 1).

Таблица 1

Откалиброванная качественная шкала оценки риска

Уровень риска	Среднегодовой ущерб в результате инцидентов безопасности (*ALE*), млн руб.
Низкие риски	
0	$0 \le ALE < 0{,}0001 \cdot Ca$
1	$0{,}0001 \cdot Ca \le ALE < 0{,}0005 \cdot Ca$
2	$0{,}0005 \cdot Ca \le ALE < 0{,}0015 \cdot Ca$
Средние риски	
3	$0{,}0015 \cdot Ca \le ALE < 0{,}003 \cdot Ca$
4	$0{,}003 \cdot Ca \le ALE < 0{,}03 \cdot Ca$
5	$0{,}03 \cdot Ca \le ALE < 0{,}1 \cdot Ca$
Высокие риски	
6	$0{,}1 \cdot Ca \le ALE < 0{,}3 \cdot Ca$
7	$0{,}3 \cdot Ca \le ALE < 0{,}5 \cdot Ca$
8	$0{,}5 \cdot Ca \le ALE$

В основу оценки ущерба может быть также положен подход, описанный в гл. 24 Уголовного кодекса Республики Беларусь. Пример калибровки шкалы с использованием данного подхода приведен в табл. 2 (при $Ca > 2000$ базовых величин).

Таблица 2

Качественная шкала оценки ущерба согласно Уголовному кодексу Республики Беларусь

Уровень ущерба (риска)	Среднегодовой ущерб в результате инцидентов безопасности (*ALE*), млн руб.
Незначительный	$0 \le ALE <$ 40 базовых величин
Значительный	40 базовых величин $\le ALE <$ 250 базовых величин
Крупный	250 базовых величин $\le ALE <$ 1000 базовых величин
Особо крупный	1000 базовых величин $\le ALE < 0{,}5 \cdot Ca$
Неприемлемый	$0{,}5 \cdot Ca \le ALE$

В качестве информационных активов, в отношении которых рассматривается угроза утечки, возьмем геологические, геофизические, геохимические и иные данные, характеризующие особенности строения и минерально-сырьевой потенциал недр, зафиксированные на материальных носителях, накопленные и обрабатываемые в ИС. Такая информация является закрытой во всех странах. Хищение данных может привести к нарушению их конфиденциальности и прав собственности. Сведения могут быть использованы физическими или юридическими лицами, которые не предусмотрены в государственных контрактах или других соглашениях (лицензиях, договорах) на производство работ по геологическому изучению недр. В результате, возможно, придется уплачивать штрафы по искам клиентов на основании заключенных с ними соглашений о конфиденциальности. Кроме того, будет нанесен ощутимый урон репутации, который выразится в сокращении числа клиентов, заказов и уменьшении коммерческой выручки.

Предположим, что согласно принятым критериям оценки финансового ущерба стоимость активов, подвергаемых угрозе утечки, $AV = 0{,}01 \cdot Ca$ млн руб. Вычислим EF и ARO.

Согласно (2) вероятность несанкционированного снятия конфиденциальной информации нарушителем четвертой категории по радиоканалу $P_{р4}$ рассчитывается по формуле

$$P_{р4} = P_4^{д} \cdot P_р^{к} \cdot P_{р4}^{н} \cdot P_р^{и}. \tag{9}$$

Вероятности $P_4^{д}$, $P_р^{к}$, $P_{р4}^{н}$, $P_р^{и}$ оценим следующим образом. Нарушитель с переносным средством технической разведки, к примеру, может посетить объект под видом сотрудника сторонней организации для проведения работ по обслуживанию инженерных коммуникаций в помещении. Перехват может осуществляться также в непосредственной близости от границы контролируемой зоны, если она недостаточно точно рассчитана. Поэтому вероятность $P_4^{д}$ равна $0,2$, если предположить, что регламентные работы проводятся еженедельно в рабочие дни. Вероятность проявления радиоканала $P_р^{к}$ равна $0,25$, т. е. составит четверть рабочего времени, в течение которого может обрабатываться информация. Вероятность доступа нарушителя к каналу при условии его доступа в зону $P_{р4}^{н}$ равна 1 (портативный приемник он имеет при себе).

Оценим вероятность наличия конфиденциальной информации в радиоканале $P_р^{и}$, т. е. вероятность выделения сигнала на фоне шума, действующего на входе приемного устройства. На практике обеспечение защиты информации от утечки по техническим каналам осуществляется с применением активной защиты – специальных широкополосных генераторов электромагнитного шума. Такие генераторы используют помехи типа «белый шум», т. е. излучают широкополосный шумовой сигнал с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот (например, гауссовский «белый шум»). Важнейшей характеристикой генератора шума является коэффициент δ – отношение сигнал-шум.

Вычислим P_o – вероятность правильного обнаружения сигнала техническими средствами разведки в пределах контролируемой зоны. При определенных допущениях вероятность P_o обнаружения сигнала с неизвестными параметрами можно рассчитать по формуле [12, 13]

$$P_o = \Phi\left[\frac{\delta \cdot \sqrt{\Delta F_{пр} T_a} - \Phi^{-1}(1 - P_{лт})}{1 + \delta}\right], \tag{10}$$

где $P_{лт}$ – вероятность ложной тревоги;

$\Delta F_{пр}$ – полоса пропускания тракта приемника, Гц;

T_a – время осреднения (анализа) процесса, с;

$T_{лт}$ – средний интервал между ложными тревогами;

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-\frac{t^2}{2}\right) dt.$$

Для обеспечения точности, достаточной для расчетов параметров перехватываемого сигнала, ошибка измерения не должна превышать 10 % от значения измеряемой величины, т. е. $P_{ош} \le 0,1 \cdot P_o$. Выбор порогового значения вероятности правильного обнаружения сигнала целесообразно осуществлять посредством минимизации вероятности полной ошибки

$$P_{ош} = P^{*}(1 - P_o) + (1 - P^{*})P_{лт}, \tag{11}$$

где P^{*} – априорная вероятность наличия сигнала на входе приемного устройства.

Подставив в формулу (11) значение вероятности полной ошибки $P_{ош} = 0,1 \cdot P_o$ для случая наибольшей неопределенности $(P^* = 0,5)$, получим $P_{оп} = 0,83$. Это означает, что при $P_o \le P_{оп}$ выделить информацию на фоне шума будет невозможно или крайне трудно.

При перехвате информации вероятности ложной тревоги составляют $10^{-6} - 10^{-3}$. Задавая пороговое значение вероятности $P_{оп}$, из формулы (10) при $\Delta F_{пр} T_a = 10, T_a \le T_{лт}$ и $P_{лт} = 10^{-3}$ получаем предельно допустимое (пороговое) значение отношения сигнал-шум на входе приемного устройства:

$$\delta_n = \frac{\Phi^{-1}(P_{оп}) + \Phi^{-1}(1 - P_{лт})}{\sqrt{\Delta F_{пр} T_a} - \Phi^{-1}(P_{оп})} = \frac{\Phi^{-1}(0,83) + 3,2}{3,16 + \Phi^{-1}(0,83)} = 1,9. \quad (12)$$

Таким образом, если $P_o \le P_{оп} = 0,83$ $(\delta \le \delta_n = 1,9)$, то перехват информации невозможен, можно только определить факт наличия или отсутствия сигнала без расчета его параметров. Поэтому вероятность наличия информации в радиоканале $P_p^и$ равна нулю.

Если $P_o > P_{оп} = 0,83$ $(\delta > \delta_n = 1,9)$, то перехват информации возможен, вероятность наличия конфиденциальной информации в радиоканале $P_p^и = P_o$.

Следовательно, вероятность несанкционированного получения конфиденциальной информации нарушителем четвертой категории по радиоканалу будет следующей:

$$P_{р4} = P_4^д \cdot P_р^к \cdot P_{р4}^н \cdot P_р^и = 0, \text{ если } \delta \le \delta_n = 1,9; \quad (13)$$

$$P_{р4} = P_4^д \cdot P_р^к \cdot P_{р4}^и \cdot P_р^и = 0,2 \cdot 0,25 \cdot 1 \cdot P_o, \text{ если } \delta > \delta_n = 1,9. \quad (14)$$

Предположим, что на объекте соблюдаются меры активной и пассивной защиты:

– границы контролируемой зоны (включающей опасные зоны R_1 и R_2) определены с учетом радиуса зоны возможного перехвата информации по результатам специальных исследований;

– осуществляется проверка импортных технических средств перед введением в эксплуатацию на отсутствие в них электронных устройств перехвата информации;

– осуществляются конструктивные доработки технических средств и помещений, где они расположены, в целях локализации возможных каналов утечки информации;

– применяются исправные адаптивные к уровню опасных сигналов генераторы шума (один генератор шума на 40 м^2, расстояние между соседними генераторами шума 20 м), которые, с одной стороны, обеспечивают гарантированную защиту информации $(\delta \le \delta_n = 1,9)$, а с другой – не засоряют эфир и не наносят вред здоровью обслуживающего персонала.

Тогда согласно (13) $EF = P_{р4} = 0$.

Из опыта можно оценить частоту реализации угрозы несанкционированного съема информации по радиоканалу (ARO): один раз в год. Следовательно, $ALE = 0,01 \cdot Ca \cdot 0 \cdot 1 = 0$ млн руб. Это минимальный уровень риска.

Если же не соблюдаются вышеперечисленные меры безопасности, некорректно рассчитаны границы контролируемой зоны, применяются неисправные или не обеспечивающие условие $\delta \le \delta_n = 1,9$ генераторы шума, то согласно (14), например, при $\delta = 2$:

$$EF = P_{р4} = 0,2 \cdot 0,25 \cdot 1 \cdot P_o = 0,2 \cdot 0,25 \cdot 1 \cdot 0,85 = 0,04.$$

Следовательно, $ALE = 0,01 \cdot Ca \cdot 0,04 \cdot 1 = 0,0004 \cdot Ca$ млн руб. Это низкий уровень риска, равный единице (см. табл. 1). Если Ca = 10 млрд руб., AV = 100 млн руб., то ALE = 4 млн руб. Согласно табл. 2 это незначительный уровень ущерба.

Аналогичным образом можно оценить риск утечки конфиденциальной информации и пороговые значения отношения сигнал-шум δ_n вследствие побочных электромагнитных излучений и наводок видеосистемы и клавиатуры компьютеров ИС.

5. Оценка риска хищения информации пользователем локальной сети, реализующей обработку геолого-геофизических данных

В качестве объекта оценки будем рассматривать приведенную выше ИС, реализующую высокопроизводительные информационно-вычислительные технологии обработки геолого-геофизических данных. Оценим риск хищения аналогичной конфиденциальной информации, к которой не был предусмотрен доступ по политике безопасности, злоумышленником из числа пользователей ИС с использованием привилегий. Особенно опасны атаки, позволяющие нарушителю получить системные права, так как в этом случае он может иметь практически полный доступ ко всем активам ИС. Это позволяет нарушителю выполнять любые несанкционированные действия по компрометации ИС, а также хищению конфиденциальных сведений.

Вероятность уязвимости оценим по методике CVSS. Уязвимости будем оценивать по наиболее широко используемым привилегиям. При вычислении оценки уязвимости, которая имеет несколько способов эксплуатации (векторов атаки), будем выбирать тот метод, который оказывает наибольшее воздействие на систему. В метрике *Au* требования аутентификации учитываются с того момента, как осуществлен доступ в систему. Для локально эксплуатируемых уязвимостей значения *S* или *M* будем присваивать, если необходима дополнительная аутентификация помимо той, которая требуется при регистрации в системе. Уязвимости, предоставляющие доступ с пользовательским уровнем привилегий, оцениваются как частичная потеря конфиденциальности, целостности и доступности.

Проанализируем базовые метрики и определим их значения: *AV* – локальный (*L* = 0,395); *AC* – высокая (*H* = 0,35) (потому что уязвимость не может произвольно эксплуатироваться злоумышленником); *Au* – многократная (*M* = 0,45) (необходима дополнительная аутентификация, помимо той которая требуется при регистрации в сети); *C, I* и *A* – частичные (*P* = 0,275). В результате получим базовый вектор $AV:L/AC:H/Au:M/C:P/I:P/A:P$.

Далее проанализируем временные метрики и определим их значения: *E* – функционально использованное (*F* = 0,95); *RL* – временное решение (*TF* = 0,90); *RC* – не подтверждена (*UC* = 0,90). В результате получим временной вектор $E:F/RL:TF/RC:UC$.

Воспользовавшись формулой (6), а также при необходимости калькулятором CVSS Calculator [14], получим *TS* = 2,6. Согласно шкале, разработанной FortiGuard Center [15] и приведенной в табл. 3, уровень опасности данной уязвимости – низкий.

Таблица 3

Шкала опасности уязвимостей FortiGuard

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

В соответствии с (7) получим $EF = \frac{2,6}{10} = 0,26.$

По формуле (8) определим вероятность использования уязвимости:

$$P_E = L \cdot H \cdot M \cdot F \cdot TF \cdot UC = 0,395 \cdot 0,35 \cdot 0,45 \cdot 0,95 \cdot 0,9 \cdot 0,9 = 0,05.$$

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

Следовательно, $ALE = 0,01 \cdot Ca \cdot 0,26 \cdot 2,6 = 0,007 \cdot Ca$ млн руб. Это средний уровень риска, равный четырем (см. табл. 1). Если Ca = 10 млрд руб., AV = 100 млн руб., то ALE = 70 млн руб. Согласно табл. 2 это крупный уровень ущерба.

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

Оценим риск хищения вышеописанной конфиденциальной информации, к которой не был предусмотрен доступ по политике безопасности, злоумышленником с использованием привилегий при ее обработке в публичной облачной системе.

Следует учитывать, что провайдеры сервисов SaaS и PaaS несут ответственность за управление конфигурацией своих платформ, а клиенты IaaS обеспечивают управление доступом к операционной системе, бизнес-приложениям и ПО уровня Middleware, безопасность конфигурации развертываемых на виртуальных серверах приложений и ПО, антивирусную защиту.

Вероятность уязвимости оценим по методике CVSS. Уязвимости, при которых обеспечивается доступ на корневом уровне, будем оценивать как полную потерю конфиденциальности, целостности и доступности. Например, нарушение целостности, которое позволяет злоумышленнику изменять файл паролей операционной системы, оценим как полное нарушение конфиденциальности, целостности и доступности. С учетом этого получим следующие результаты.

Базовые метрики принимают значения: 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 $AV:N / AC:L / Au:S / C:C / I:C / A:C$.

Временные метрики принимают значения: E – высокое (H = 1,0); RL – официальное исправление (OF = 0,87); RC – подтверждена (C = 1,0). Получим временной вектор $\mathrm{E:H/\ RL:OF/\ RC:C}$. Следовательно, по формуле (6) получим TS = 7,8, что согласно табл. 3 соответствует высокому уровню опасности. После нормирования получим EF = 0,78.

По формуле (8) определим вероятность использования уязвимости:

$$P_E = N \cdot L \cdot S \cdot H \cdot OF \cdot C = 1,0 \cdot 0,71 \cdot 0,56 \cdot 1,0 \cdot 0,87 \cdot 1,0 = 0,35.$$

В предположении, что пользователь еженедельно имел возможность осуществлять несанкционированный доступ с использованием привилегий, получим $ARO = 52 \cdot 0,35 = 18,2$. Следовательно, $ALE = 0,01 \cdot Ca \cdot 0,78 \cdot 18,2 = 0,14 \cdot Ca$ млн руб. Это высокий уровень риска, равный шести (см. табл. 1). Если Ca = 10 млрд руб., AV = 100 млн руб., то ALE = 1400 млн руб. Согласно табл. 2 это особо крупный уровень ущерба. В случае если имеются более подробные сведения об ИС и облачной системе, то полученные временные оценки можно улучшить путем использования контекстной формулы, в которой метрики среды объединяются с временной оценкой. В конечном итоге учет показателей временной метрики позволит уменьшить вероятность успешного применения уязвимости.

Справедливость расчетов по оценке вероятностей использования уязвимостей для локальной ИС и облачной системы подтверждается статистическими данными. В [16] отмечается, что по вектору эксплуатации уязвимости распределились следующим образом: 77 % уязвимостей эксплуатировались удаленно, 15 % уязвимостей – по локальной сети, 8 % уязвимостей требовали физического доступа. Полученная оценка возможного риска для облачных вычислений показывает, что использование публичного облака неприемлемо в случае обработки конфиденциальной информации, для этой цели может использоваться, например, гибридное облако или следует применять криптографическую защиту конфиденциальной информации.

Заключение

В статье предложен метод оценки рисков утечки конфиденциальной информации на основании методик GlobalTrust и CVSS. Проведены оценки рисков утечки конфиденциальной информации по радиоканалу, а также хищения конфиденциальных сведений, к которым не был предусмот-

рен доступ по политике безопасности, для различных типов развертывания информационных систем. Уровень риска утечки конфиденциальной информации по радиоканалу при конкретной структуре ИС и стоимости активов оценен как низкий, а уровень риска хищения конфиденциальной информации пользователем локальной сети – как средний. Для сравнения, уровень риска хищения конфиденциальной информации, обрабатываемой в публичном облаке, оценен как высокий. Другими словами, при одних и тех же условиях риск хищения конфиденциальной информации в публичном облаке примерно в 20 раз выше, чем в локальной сети.

Полученные результаты позволяют оценить реальные возможности перехвата информации средствами технической разведки и обосновать целесообразность использования тех или иных средств защиты от утечки информации по техническим каналам. Кроме того, можно сделать вывод о необходимости применения дополнительных средств защиты конфиденциальной информации, например гомоморфного шифрования [17], при ее обработке в публичном облаке.

Список литературы

1. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования : СТБ ISO/IEC 27001–2011. – Минск : Госстандарт, 2011. – 28 с.

2. Домнич, К. Беларусь в международном исследовании компании EY по информационной безопасности за 2013 год / К. Домнич, А. Ворошилов // Банкаўскі веснік. – 2014. – № 2. – С. 64–67.

3. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3 «О внесении дополнений и изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62» [Электронный ресурс]. – 2015. – Режим доступа : http://www.oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_3.htm. – Дата доступа : 06.04.2015.

4. Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности : СТБ ISO/IEC 27005–2012. – Минск : Госстандарт, 2012. – 61 с.

5. Information technology – Security techniques – Information security incident management : ISO/IEC 27035:2011. – Geneva : ISO/IEC, 2011. – 78 p.

6. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach : NIST 800–37:2010. – Gaithersburg : NIST, 2010. – 93 p.

7. Малюк, А.А. Теория защиты информации / А.А. Малюк. – М. : Горячая линия – Телеком, 2013. – 184 с.

8. Астахов, А.М. Искусство управления информационными рисками / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с.

9. Common Vulnerability Scoring System (CVSS-SIG) [Electronic resource]. – 2015. – Mode of access : http://www.first.org/cvss. – Date of access : 06.04.2015.

10. Система оценки общеизвестных уязвимостей. Рекомендация. МСЭ-Т X.1521 (04/2011) [Электронный ресурс]. – 2015. – Режим доступа : https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1521-201104-I!!PDF-R&type=items. – Дата доступа : 06.04.2015.

11. Малюк, А.А. Один из подходов к оценке рисков информационной безопасности в облачных средах / А.А. Малюк, А.В. Царегородцев, Е.В. Макаренко // Безопасность информационных технологий. – 2014. – № 4. – С. 68–74.

12. Хорев, А.А. Оценка возможностей средств радиоразведки по перехвату информации / А.А. Хорев // Специальная техника. – 2009. – № 2. – С. 54–63.

13. Трубей, А.И. Статистические и нейросетевые методы оценки эффективности защиты информации, обрабатываемой средствами вычислительной техники / А.И. Трубей, В.А. Дмитриев, В.В. Анищенко // Электроника инфо. – 2013. – № 6. – С. 24–26.

14. NVD Common Vulnerability Scoring System Support v.2 [Electronic resource]. – 2015. – Mode of access : http://www.nvd.nist.gov/cvss.cfm?calculator&version=2. – Date of access : 06.04.2015.

15. Vulnerability Severity Level [Electronic resource]. – 2015. – Mode of access : http://www.fortiguard.com/static/intrusionprevention.html. – Date of access : 06.04.2015.

16. Статистика уязвимостей в 2011 году [Электронный ресурс]. – 2015. – Режим доступа : http://www.securitylab.ru/analytics/422328.php. – Дата доступа : 06.04.2015.

17. Трубей, А.И. Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор) / А.И Трубей // Информатика. – 2015. – № 1. – С. 90–101.

Поступила 17.04.2015

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: trubeia@newman.bas-net.by

A.I. Trubei

INFORMATION SECURITY RISK ASSESSMENT USING EXISTING LEGAL AND METHODOLOGICAL BASE

The article provides a survey of the existing regulatory framework for information security risk management. Practical methods for information security risk and vulnerability assessment are proposed.