DOI: 10.18372/2410-7840.21.13445
УДК 004.621:681.324

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ПО КРИТЕРИЮ УВЕРЕННОСТИ

Юрий Самохвалов, Николай Браиловский

В настоящее время защита информации остается актуальной проблемой, а наиболее распространенными подходами к ее оценке являются верификационный и риск-ориентированный. Однако, метрики информационной безопасности (ИБ) в соответствующих методиках, основанных на этих подходах недостаточно информативны, так как учитывают лишь объективные аспекты безопасности, совершенно игнорируя субъективные. Поэтому они не позволяют выработать основные суждения о состоянии конфиденциальности, целостности и доступности информации и уровне ИБ организации в целом. В связи с этим возникает необходимость в разработке методического аппарата оценки ИБ организации с учетом объективных и субъективных аспектов безопасности. В статье предлагается подход к оценке ИБ на основе критерия уверенности в том, что в организации реализуется принятая политика безопасности. Оценка уверенности включает оценку доверия к информационной безопасности организации, качества модели оценки доверия и бекграунда лиц, проводивших такую оценку и оценку знаний относительно угроз. В качестве показателя уверенности используется показатель полезности как значение обобщенной функции желательности Харрингтона. Предложенный подход к оценке ИБ организации является довольно простым в реализации и может быть использован в качестве пилотажа для разработки соответствующих методик оценки ИБ организаций различных форм собственности.

Ключевые слова: *оценка, информационная безопасность, уверенность, доверие, функция Харрингтона, модель зрелости.*

1. Введение. В последнее время конфиденциальная для бизнеса информация все больше входит в сферу повышенного интереса конкурирующих компаний, так как известно, кто владеет информацией о конкурентах, тот получает беспрецедентные преимущества в борьбе с ними. Поэтому вопрос информационной безопасности (ИБ) в настоящее время становится краеугольным камнем в деятельности практически любой организации. Как любил говорить У. Черчилль "За безопасность необходимо платить, а за ее отсутствие – расплачиваться".

На сегодняшний день не выработано единого подхода к интерпретации понятия «информационная безопасность». Учитывая множественность дефиниций безопасности в статье под информационной безопасностью, согласно стандарта ISO/IEC 27000:2009 [1], понимается состояние защищенности информации, при котором обеспечены ее конфиденциальность, целостность и доступность.

В действующей практике можно выделить следующие основные типы метрик информационной безопасности [2]: метрики реализации, служащие для измерения степени проведения политики безопасности в жизнь; метрики эффективности, служащие для измерения результативности сервисов безопасности. Эти метрики являются основой наиболее распространенных в настоящее время подходов к оценке защищенности информации: верификационного и риск-ориентированного. Верификационный подход основан на сравнении деятельности и мер по обеспечению ИБ организации с требованиями стандартов или руководящих документов в области информационной безопасности и защиты информации. В результате формируется оценка степени соответствия ИБ требованиям заданных эталонов. Риск-ориентированный подход связан с оценкой и управлением рисками или риск-менеджментом. Он предполагает учет всех возможных факторов угроз информационной безопасности, вероятности их реализации (атак или инцидентов) и ценности защищаемых информационных активов. В результате будет сформирована оценка способности организации эффективно управлять рисками ИБ для достижения своих целей.

При этом данные подходы обладают общим недостатком: полученные в результате применения методик метрики информационной безопасности недостаточно информативны, так как учитывают лишь объективные аспекты безопасности, совершенно игнорируя субъективные. Поэтому они не позволяют выработать обоснованные суждения о состоянии конфиденциальности, целостности и доступности информации и уровне ИБ организации в целом [3, 4].

В стандарте ISO/IEC TR 15443-1:2005 [5] впервые вводится субъективная категория ИТ-безопасности «доверие». Также приводятся методы обеспечения доверия. Эти методы могут быть специфичными для конкретной стадии жизненного

цикла объекта доверия, в соответствии со стандартами серии ISO 9000, ISO/IEC 15408-1:2009 [6] и стандартом SSE-CMM (ISO/IEC 21827:2008) [7]. В работах [8, 9] предложены модели оценки доверия к информационной безопасности, а в [10] рассмотрены примеры организации и использования мер обеспечения уверенности и доверия на основе требований стандарта [11]. Однако рассмотренные примеры не позволяют использовать их на практике для оценки ИБ. Кроме этого в [12] обосновывается использование конфиденциальности в качестве субъективного показателя допустимого уровня защищенности информации. В статье предложен альтернативный подход к оценке ИБ с учетом объективных и субъективных аспектов безопасности. Это положение определяет *цель и основное содержание данной статьи.*

2. Категории уверенности и доверия. С объективной точки зрения безопасность может быть детерминирована состоянием ее объекта, наличием или отсутствием у него определенных свойств, способностей и т.д. С субъективной же точки зрения безопасность определяется как некое чувство, ощущение, осознание, восприятие ее субъекта [13]. Причем именно субъективная трактовка понятия «безопасность» доминирует в обыденном сознании, подтверждением чему служат результаты исследования [14]: из 1506 респондентов на вопрос, как они чаще всего понимают «безопасность» 234 ответили - как «спокойствие», 185 – как «уверенность» и 128 – как «покой».

Оценка безопасности может быть получена разными методами. Однако какой бы метод не использовался, такая оценка будет носить субъективный характер, так как субъективен выбор пороговых значений индикаторов безопасности, субъективны экспертные оценки, субъективна оценка рисков ИБ. Таким образом, объект получает статус «опасный» или «безопасный» лишь в результате оценочной деятельности человека, что служит еще одним подтверждением необходимости учета субъективных аспектов в определении понятия «безопасность».

Информационная безопасность организации, как состояние защищённости информационной среды, непосредственно зависит от защищенности ее информационной инфраструктуры, которая, как показывает практика, является основным источником уязвимостей и угроз ИБ. А так как с появлением новых информационных технологий появляются как новые уязвимости, так и новые атаки, то очевидно, что ошибки, уязвимости и риски всегда будут существовать. Поэтому почти невозможно гарантировать безопасность функционирования организации. В данной ситуации мы можем только утверждать с некоторой степенью уверенности, что организация осуществляет (реализует) принятую политику безопасности. А это в свою очередь индуцирует применение соответствующих технических и организационных мер безопасности для ослабления уязвимостей и угроз с целью обеспечения достаточно приемлемого уровня доверия к ИБ организации.

Следует отметить, что "доверие" и "уверенность" не являются идентичными и взаимозаменяемыми. С позиций психологии, как отмечено в стандарте [5], уверенность в ИБ организации с точки зрения отдельного индивидуума связана с убеждением, что он обладает доверием к ее ИБ, тогда как доверие связано с доказанной способностью системы ИБ организации обеспечивать выполнение ее цели безопасности. Таким образом, уверенность является выражением убежденности, полученной через оценку доверия.

Доверие определяется свидетельством, полученным в результате оценки объекта. Свидетельство, обычно включающее в себя аргумент доверия, документацию и другие соответствующие рабочие материалы, служит основанием для утверждения доверия, которое основано на результатах действий, связанных с проектированием и оценкой безопасности.

Уверенность является предметом восприятия отдельным лицом специфических требований безопасности и информации, полученной в результате оценки, о том, что оцениваемый объект будет функционировать в соответствии с установленными требованиями. Уверенность подразумевает знание критериев, метода, системы обеспечения доверия и используемых процедур оценки. При этом уверенность основывается на знаниях того, что известные нам опасности не имеют на нас каналов влияния или же они минимизированы (предпринята защита), и мы знаем способности этой защиты, или же ничтожна вероятность возможных опасностей. Относительно же неизвестных опасностей мы имеем систему, которая способна их прогнозировать или же выявлять их и адекватно под них подстраиваться. Кроме этого важным фактором формирования уверенности также является репутация, квалификация и опыт специалистов, проводящих оценку. В результате индивидуального восприятия у разных людей могут возникнуть различные степени уверенности в результате использования соответствующего метода обеспечения доверия как отдельным лицом, так и организацией в целом.

Согласно [5] следует различать доверие корректности (правильности) и доверие эффективности. Доверие правильности связано с оценкой соответствия ИБ организации требованиям стандартов или передовым мировым практикам в области информационной безопасности и защиты информации. Напротив, доверие к эффективности относится к способности функций (процессов) безопасности противостоять осознанным или идентифицированным угрозам. Как доверие к корректности, так и доверие к эффективности являются важными характеристиками, и ни одна из них не обладает преимуществом, поскольку оба типа доверия оперируют значимыми аспектами объекта.

В этом стандарте в частности отмечается: «Если функциональные возможности обеспечения безопасности объекта учитывают потенциальные угрозы и эти возможности не были проанализированы относительно установления корректности и реализации проекта, то нельзя быть уверенным в успехе противостояния объекта атаке. Аналогично, если анализ установил корректность проекта и правильность реализации функциональных возможностей обеспечения безопасности объекта, а в проекте не предусмотрены соответствующие функции безопасности для противостояния вероятным угрозам, то нельзя быть уверенным, что объект устоит перед этими угрозами.

С целью получения общего доверия объект должен быть оценен на предмет корректности проекта, внедрения и эксплуатации (элемент корректности) и должен обладать соответствующими функциональными возможностями обеспечения безопасности для противостояния идентифицированным угрозам (элемент эффективности)». Поэтому на практике необходима комбинация данных мер доверия к безопасности. с целью получения общего доверия к ИБ организации, которое будет служить основой нашей уверенности, что организация реализует принятую политику безопасности.

3. Модель оценки информационной безопасности. Важнейшим назначением оценки ИБ организации является создание информационной потребности для совершенствования ее ИБ. При этом целью проведения оценки ИБ является определение степени уверенности, с которой в организации реализована политика безопасности.

Как было отмечено, уверенность в ИБ организации основывается на:

– доверии к ИБ, качестве модели оценки доверия и бэкграунде лиц, проводимых оценку доверия;

– знаниях, что известные угрозы не имеют каналов влияние на бизнес-процессы или они минимизированы (предпринята защита) и мы знаем способности этой защиты, или же ничтожна вероятность возможных угроз;

– знаниях, что относительно неизвестных угроз имеются средства, которые способны их прогнозировать или выявлять.

Для наглядности эти факторы можно представить следующим графом (рис. 1).

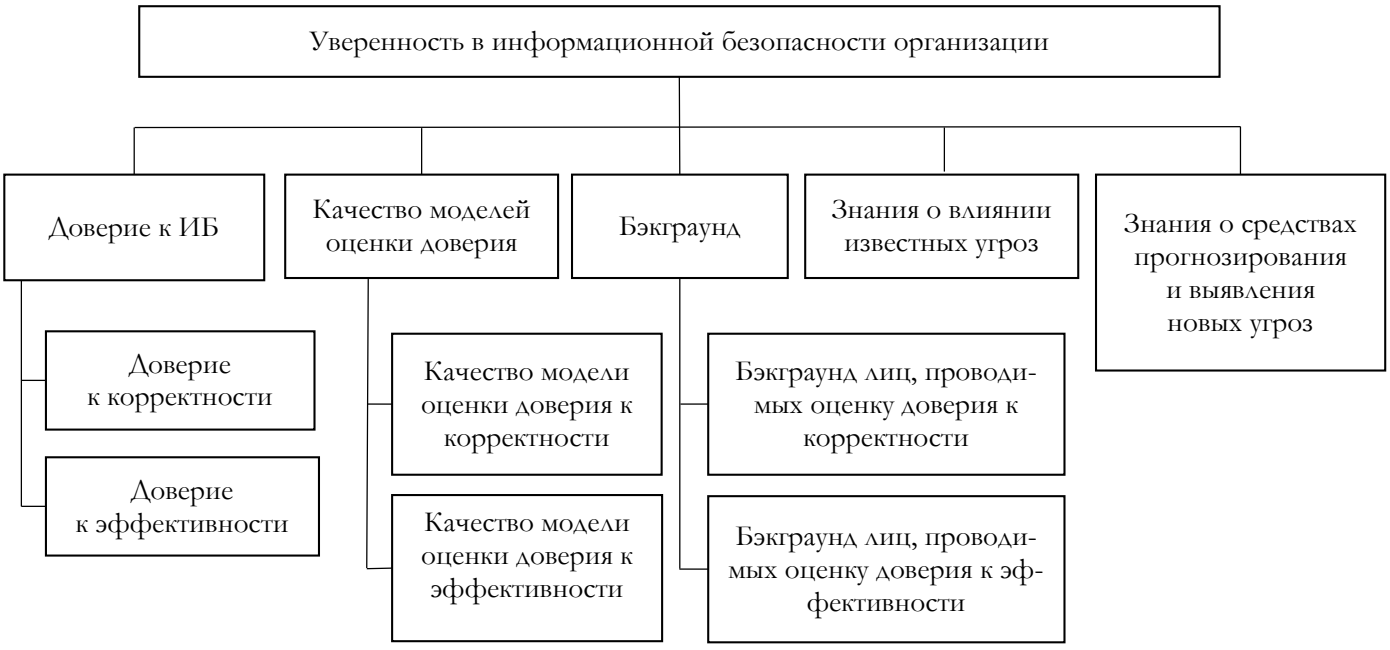

Рис. 1. Граф факторов формирования уверенности

Здесь под бэкграундом следует понимать репутацию, квалификацию и опыт специалиста.

Введем обозначения:

– U – уверенность в ИБ организации;

– C – доверие к ИБ организации;

– C_k – доверие к корректности;

– $C_э$ – доверие к эффективности;

– P – качество процедур оценки доверия;

– P_k – качество процедур оценки доверия к корректности;

– $P_э$ – качество процедур оценки доверия к эффективности;

– B – бэкграунд лиц, проводимых оценку доверия;

– B_k – бэкграунд лиц, проводимых оценку доверия к корректности;

– $B_э$ – бэкграунд лиц, проводимых оценку доверия к эффективности;

– Z – знания относительно угроз;

– R – знания относительно влияния известных угроз;

– F – знания относительно прогнозирования и выявления новых угроз.

Тогда формирование уверенности в ИБ организации можно представить в виде отображения

$$\Re : (C, P, B, Z) \to U , \qquad (1)$$

в котором объекты C, P, B, Z в свою очередь являются отображениями вида:

$$\Re_C : (C_k, C_э) \to C ,$$
$$\Re_P : (P_k, P_э) \to P , \ \Re_B : (B_k, B_э) \to B , \qquad (2)$$
$$\Re_Z : (R, F) \to Z .$$

Если отождествить данные отображения с соответствующими задачами, то оценка ИБ организации заключается в решении пяти взаимосвязанных и взаимообусловленных задач: оценки уверенности в ИБ организации, оценки доверия к ИБ, измерения качества процедур оценки доверия, оценки бэкграунда лиц, проводимых оценку доверия и оценки знаний относительно влияния известных угроз и прогнозирования и выявления новых. При этом основная проблема, которая возникает при решении этих задач это выбор соответствующего показателя и способа его вычисления.

Одним из основных принципов, которым необходимо руководствоваться при выборе критериев оценки ИБ, является безусловное отражение критерием полезности для организации с точки зрения конфиденциальности, целостности и доступности информации [15]. Поэтому в качестве критерия оценки ИБ предлагается использовать уверенность, так как она является выражением убежденности, что система ИБ организации обеспечивает данные сервисы безопасности, а в качестве показателя уверенности – обобщенную функцию желательности Харрингтона [16]. Это позволит использовать единую универсальную психофизическую шкалу измерения, которая полностью корреспондируется с законом Вебера-Фехнера о нелинейности шкал измерений субъективных суждений [17, 18]. В табл. 1 приведена вербально-числовая шкала Харрингтона, которая устанавливает соответствие между натуральными значениями показателей в физических шкалах и психофизическими параметрами – субъективными лингвистическими оценками «желательности (полезности)» этих значений для человека.

Таблица 1

Лингвистическая оценка желательности	Интервалы значений функции желательности
Очень высокая	0,8 – 1,0
Высокая	0,63 – 0,8
Удовлетворительная	0,37 – 0,63
Низкая	0,2 – 0,37
Очень низкая	0,0 – 0,2

При этом нижняя граница каждого интервала значений включается в соответствующий интервал.

Вопросы построение обобщенной функции желательности Харрингтона детально рассмотрены в [19], поэтому они опускаются. Отметим только, что мы будем использовать функцию желательности Харрингтона с односторонним ограничением, которая задается формулой:

$$d_i = \exp(-\exp(-y_i^н)) , \qquad (3)$$

где $y_i^н$ – нормированное значение показателя y_i, d_i – частная желательность.

При этом значения $y_i^{'}$ вычисляются по формуле:

$$y_i^{'} = -2 + 7 \cdot (y_i - y_{\min})/(y_{\max} - y_{\min}) , \qquad (4)$$

где $y_{\min}$ и $y_{\max}$ – нижняя и верхняя границы области изменения показателя y_i.

После вычисления частных желательностей d_i осуществляется их свертка в обобщенный показатель D – обобщенная функция желательности. Эта функция задается формулой

$$D = \sqrt[n]{\prod_{i=1}^{n} d_i} . \qquad (5)$$

Для обобщенного показателя D используется та же шкала желательности (табл. 1).

4. Оценка доверия к ИБ организации. Согласно (2) доверие C к ИБ основывается на доверии C_k к корректности реализации процессов и защитных мер и доверии $C_э$ к эффективности процессов информационной безопасности.

Оценка доверия к корректности (правильности) процессов и защитных мер. Доверие к корректности (правильности) процессов и защитных мер сводится к оценке степени их соответствия требованиям эталону, в качестве которого взят стандарт СТО БР ИББС-1.0-2014 [20]. Этот стандарт (как семейство стандартов) выбран в качестве базового так как он, на наш взгляд, во-первых, впитал требования и рекомендации международных стандартов и передовых мировых практик о области информационной безопасности, а во-вторых, содержит методические рекомендации по оценке ИБ, которые можно применить для организаций различных форм собственности. При необходимости этот стандарт может быть дополнен национальными стандартами в области ИБ, а также требованиями и рекомендациями отраслевых нормативных документов по обеспечению ИБ.

Для оценки уровня соответствия ИБ требованиям этого стандарта используются групповые и частные показатели ИБ. Групповые показатели ИБ отражают области обеспечения ИБ организации, а частные − требования этого стандарта, предъявляемые по каждой из областей. С помощью частных показателей оцениваются различные по своей природе атрибуты процессов обеспечения ИБ, что дает возможность оценить уровня выполнения требований данного стандарта. Интегральная оценка выполнения требований стандарта [20] формируется из оценок групповых показателей ИБ.

Пусть $O = \{o_i \,|\, i = \overline{1,m}\}$ − множество областей обеспечения ИБ; $T_i = \{t_{ij} \,|\, j = \overline{1,n_i}\}$ − множество требований стандарта, предъявляемые к i-й области. Измерение степени выполнения требований t_{ij} будем осуществлять с помощью шкалы Харрингтона. В результате будут получены частные оценки d_{ij} правильности (желательности) реализации этих требований. Тогда групповой показатель D_i, отражающий правильность реализации требований, предъявляемые к i-й области обеспечения ИБ, вычисляется по формуле:

$$D_i = \sqrt[n_i]{\prod_{j=1}^{n_i} d_{ij}}\ , \qquad (6)$$

а интегральная оценка по формуле:

$$C_k = \sqrt[m]{\prod_{i=1}^{m} D_i}\ . \qquad (7)$$

Эта оценка отражает степень доверия к правильности реализации процессов и защитных мер обеспечения ИБ организации требованиям стандарта [20].

Оценка доверия к эффективности процессов информационной безопасности. Доверие к эффективности процессов информационной безопасности базируется на требованиях к составу и модели зрелости процессов информационных технологий, которые получили широкое распространение в области ИБ. В [21] приведен сравнительный анализ наиболее распространенных и часто используемых моделей зрелости, а именно:

– Open Information Security Management Maturity Model (O-SIM3);

– Process Capability Model(PCM);

– Business Process Management Maturity Model (BPM MM);

– Community Cyber Security Maturity Model (CCSMM).

Анализ показывает, что ни одна из рассмотренных моделей в полной мере не отражает всех современных требований по ОИБ для организаций различного размера и сферы деятельности. Поэтому организации следует подобрать и применить под свои потребности, а, возможно, и разработать собственную модель зрелости с подходящими для нее метриками, используя рассмотренные модели в качестве образца. Вместе с тем, модель PCM [22] по сравнению с другими, во-первых, имеет рекомендательный, а не описательный характер. Во-вторых, она ориентирована на ИТ-инфраструктуру и, в-третьих, рекомендуемая стандартом [20] в организациях банковской сферы. С учетом сказанного эту модель будем использовать в качестве эталонной модели зрелости процессов ИБ.

Модель зрелости PCM является мерой оценки полноты, адекватности и эффективности процессов менеджмента ИБ. Эта модель определяет шесть уровней зрелости с нулевого по пятый. Уровень зрелости процессов ИБ определяется тем, насколько полно и последовательно менеджмент организации руководствуется принципами ИБ, реализует политики и требования ИБ, использует накопленный опыт и совершенствует системы менеджмента информационной безопасности.

Модель зрелости процессов менеджмента ИБ организации определяет шесть уровней зрелости организации – с нулевого по пятый. Оценку уровня зрелости процессов ИБ будем проводить согласно методологии ISF (Information Security Forum), которую компании PwC широко применяют для оценки зрелости процессов ИБ в организациях. Оценке подлежат 21 процесс ИБ, описанный с учетом наиболее известной международной практики и общепринятых стандартов (ISO27000, COBIT5 for Information Security, SANS, NIST и т. д.) [23] (табл. 3).

Оценку уровня зрелости процессов ИБ будем проводить по следующей шкале (табл. 4).

Таблица 3

№ процесса	Наименование процесса ИБ
1	Стратегия ИБ
2	Осознание руководством важности ИБ
3	Управление рисками И Б
4	Управление комплаенсом
5	Аудит ИБ
6	Политика ИБ
7	Управление доступом
8	Управление уязвимостями
9	Управление ЖЦ АС
10	Управление информационными активами
11	Управление изменениями
12	Архитектура ИБ
13	Управление каналами связи
14	Управление внешним взаимодействием
15	Разведка угроз ИБ
16	Управление событиями ИБ
17	Управление инцидентами ИБ
18	Антикризисное управление
19	Обеспечение непрерывности бизнеса
20	Повышение осведомленности персонала
21	Безопасность персонала

Таблица 4

Уровень	Обозначение уровня зрелости	Описание
0	Несуществующий	Процесс ИБ не выполняется
1	Примитивный	Процесс ИБ выполняется на нерегулярной основе
2	Начальный	Процесс ИБ выполняется на регулярной основе и поддерживается на уровне планирования (включая привлечение заинтересованных сторон и использование соответствующих стандартов и руководств)
3	Формализованный	Процесс ИБ выполняется, планируется, и имеется достаточный объем организационных ресурсов для поддержки и управления
4	Управляемый	Процесс ИБ выполняется, планируется, управляется и контролируется
5	Оптимизированный	Процесс ИБ выполняется, планируется, управляется, измеряется при помощи количественных показателей (метрик) и постоянно совершенствуется

Эта шкала предлагает способ оценки «от начального к максимальному», заключающийся в поглощении требований предыдущего уровня зрелости последующим. Например, процесс соответствует второму уровню зрелости только в случае, если выполняют все требования для первого уровня.

Пусть $PR = \{p_i \mid i = \overline{1,21}\}$ – множество процессов ИБ, y_i – оценка зрелости i-го процесса, а $y_i^н$ – нормированное значение оценки y_i, вычисленное согласно (4) по формуле:

$$y_i^н = -2 + 7 \cdot (y_i - y_{\min}) / (y_{\max} - y_{\min}), \qquad (8)$$

где $y_{\min} = 0$ и $y_{\max} = 5$.

Тогда частная желательность d_i процесса p_i вычисляется по формуле (3):

$$d_i = \exp(-\exp(-y_i^n)), \quad (9)$$

а оценка $C_э$ доверия к эффективности процессов информационной безопасности организации вычисляется по формуле:

$$C_э = \sqrt[21]{\prod_{i=1}^{21} d_i}. \quad (10)$$

И, наконец, оценка доверия к ИБ организации определяется значением функции:

$$D_C = \sqrt{C_k \cdot C_э}. \quad (11)$$

5. Измерение качества модели оценки доверия и бекграунда. Как следует из выше сказанного оценка доверия является результатом экспертизы. Следовательно, качество модели оценки доверия в данном случае зависит от того, в какой мере экспертный метод и процедура его реализации обеспечивает объединение математических моделей и оценочных суждений экспертов с целью получения достоверного результата. Исходя из этого качества модели оценки доверия можно представить кортежем:

$$< M, L >,$$

где M – экспертный метод, L – процедура его реализации.

Оценивать эти атрибутов будем по шкале Харрингтона с точки зрения их полезности. Пусть ξ_{M_k}, ξ_{L_k} и $\xi_{M_э}$, $\xi_{L_э}$ – оценки полезности экспертного метода и процедуры его реализации получения оценок доверия C_k и $C_э$ соответственно. Тогда оценки P_k и $P_э$ качества моделей оценки доверия к корректности и эффективности вычисляется по формулам:

$$P_k = \sqrt{\xi_{M_k} \cdot \xi_{L_k}} \text{ и } P_э = \sqrt{\xi_{M_э} \cdot \xi_{L_э}}, \quad (12)$$

а качество модели оценки доверия к ИБ по формуле:

$$D_P = \sqrt{P_k \cdot P_э}. \quad (13)$$

Оценку бекграунда лиц, проводивших оценку доверия к ИБ, также будем давать по шкале Харрингтона. Пусть ξ_{B_k} и $\xi_{B_э}$ – оценки бекграунда лиц, проводивших оценку доверия к корректности и эффективности. Тогда оценка бекграунда лиц, проводивших оценку доверия к ИБ можно получить по формуле:

$$D_B = \sqrt{\xi_{B_k} \cdot \xi_{B_э}}. \quad (14)$$

При этом заметим, что для получения более точных оценок ξ_{B_k} и $\xi_{B_э}$ можно использовать один из методов многокритериальной оценки квалификации экспертов, рассмотренных в [24].

6. Оценка знаний относительно угроз. Знания относительно угроз (Z) можно охарактеризовать полнотой и достоверностью информации (свидетельствами) относительно того, что, во-первых, известные угрозы не имеют каналов влияние на бизнес-процессы или они минимизированы (предпринята защита) и мы знаем способности этой защиты, или же ничтожна вероятность возможных угроз (R). А во-вторых, что имеются средства, способны прогнозировать или выявлять новые угрозы (F). Под достоверностью информации будем понимать ее свойство отражать объективную реальность с необходимой точностью. Тогда зная достоверность имеющейся информации относительно угроз и учитывая полноту свидетельств, по шкале Харрингтона можно определить полезность этих знаний как фактора обеспечения уверенности.

Пусть d_R, d_F – оценки полезности знаний R и F. Тогда оценка полезности знаний Z в целом вычисляется по формуле:

$$D_Z = \sqrt{d_R \cdot d_F}. \quad (15)$$

При оценке достоверности информации согласно [25] будем использовать схему Кента [26, 27], которая дает наглядную классификацию информации с точки зрения степени ее достоверности (рис. 3).

Пусть ξ_R, ξ_F – оценки достоверности свидетельств знаний R и F. Тогда оценки d_R, d_F можно получить используя формулы (3) и (4).

И, наконец, степень D_U уверенности, с которой в организации реализована политика безопасности определяется значением функции:

$$D_U = \sqrt[4]{D_C \cdot D_P \cdot D_B \cdot D_Z}. \quad (16)$$

7. Практическая реализация. Рассмотрим пример, иллюстрирующий предлагаемый подход к оценке ИБ организации. С целью обеспечения всестороннего анализа и объективности оценок в качестве экспертов целесообразно привлекать руководителей служб информационной безопасности в организациях.

А. Оценка доверия к ИБ организации. Как было отмечено, доверие к ИБ основывается на доверии к корректности реализации процессов и защитных мер и доверии к эффективности процессов информационной безопасности.

Оценку доверия к корректности (правильности) процессов и защитных мер будем давать с помощью групповых и частных показателей ИБ. В качестве групповых показателей выступают соответствующие области обеспечения ИБ (табл. 5).

Каждой области обеспечения ИБ, согласно [20], соответствует список частных показателей оценки. С целью сокращения объема статьи рассмотрим, например, только 4-ю и 6-ю области обеспечение ИБ и первые 4 частных показателя, которые соответствуют данным областям.

Оценка частных показателей осуществляется по методике, включающей анкеты-вопросники с использованием шкалы Харрингтона, а групповые показатели вычисляются по формуле (6). Соответствующие оценки приведены в табл. 6 и 7.

ДОСТОВЕРНОСТЬ					
Шансы за			Шансы против	Степень достоверности, выраженная в шансах	Степень достоверности, выраженная через понятия вероятности
Степень достоверности	99 85		1 15	Почти определенно, информация достоверная (шансы: за – 9, против – 1)	Почти определенно, информация достоверная (почти определенно - да)
	84 60		16 40	Имеется много шансов, что информация достоверная (шансы: за – 3, против – 1)	Вероятно, информация достоверна (вероятно – да)
	59 40		41 60	Шансы примерно равны (шансы: за – 1, против – 1)	
	39 15		61 85	Имеется много шансов, что информация недостоверна (шансы: за – 1, против – 3)	Вероятно, информация недостоверна (вероятно – нет)
	14 1		86 99	Почти определенно, информация недостоверна (шансы: за – 1, против – 9)	Почти определенно, информация недостоверна (почти определенно - нет)
НЕДОСТОВЕРНОСТЬ					

Рис. 3. Схема Кента, иллюстрирующая степень достоверности информации

Таблица 5

№	Области обеспечения ИБ
1	Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу;
2	Обеспечения ИБ на стадиях жизненного цикла ИС организации;
3	Обеспечение ИБ при управлении доступом и регистрацией;
4	Обеспечение ИБ средствами антивирусной защиты;
5	Обеспечение ИБ при использовании ресурсов сети Интернет;
6	Обеспечение ИБ при использовании средств криптографической защиты информации;
7	Обеспечение ИБ технологических процессов;
8	Обеспечение ИБ информационных технологических процессов;
9	Обработка персональных данных в организации;
10	Обеспечение ИБ технологических процессов, в рамках которых обрабатываются персональные данные.

В результате, оценка доверия к корректности (правильности) процессов и защитных мер согласно (7) равна:

$$C_K = \sqrt{D_1 \cdot D_2} = \sqrt{0,78 \cdot 0,85} = 0,81.$$

Оценка доверия к эффективности процессов информационной безопасности. Такая оценка проводиться для всех процессов, представленные в табл.3 по шкале (табл. 4). Для анализа должны быть использованы следующие свидетельства [9]:

– документальные свидетельства выполнения оценки потенциальных потерь (ущерба) бизнесу организации в результате воздействия (возможной реализации) угроз информационной безопасности;

– документальные свидетельства выбора варианта минимизации (обработки) рисков применительно ко всем рискам, оцененным после выполнения процесса;

– документальные свидетельства снижения количества потенциальных инцидентов, вызванных рисками и выявленных постфактум;

– документальные свидетельства увеличения количества выявленных рисков, влияние которых было ослаблено.

Результаты оценки приведены в табл. 8, в которой значения y_i, y_i'' и d_i получены соответственно по шкале Харрингтона и формулам (8) и (9).

Таблица 6

Номер показателя	Частные показатели обеспечение ИБ средствами антивирусной защиты	Оценка частного показателя d_{1j}
1	Применяются ли на всех автоматизированных рабочих местах и серверах ИС организации, если иное не предусмотрено технологическим процессом, средства антивирусной защиты?	0,83
2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах ИС?	0,68
3	Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных?	0,95
4	Проводится ли антивирусная проверка съемных носителей информации перед их подключением к средствам вычислительной техники, задействованным в рамках осуществления банковских технологических процессов, на специально выделенном автономном средстве вычислительной техники?	0,7
Оценка группового показателя D_1		0,78

Таблица 7

Номер показателя	Частные показатели обеспечение ИБ при использовании средств криптографическойзащиты информации	Оценка частного показателя d_{2j}
1	Проводится ли применение СКЗИ в организации в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией?	0,87
2	Имеют ли СКЗИ, применяемые для защиты персональных данных, класс не ниже КС2?	0,92
3	Проводятся ли работы по обеспечению безопасности информации с помощью СКЗИ в соответствии с действующими законодательством, нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями?	0,74
4	Утверждена ли частная политика, касающаяся применения СКЗИ в организации?	0,88
Оценка группового показателя D_2		0,85

Таблица 8

№ домена	Наименование процесса ИБ	y_i	$y_i^н$	d_i
1	Стратегия ИБ	4	3,6	0,973
2	Осознание руководством важности ИБ	3	2,2	0,895
3	Управление рисками ИБ	4	3,6	0,973
4	Управление комплаенсом	4	3,6	0,973
5	Аудит ИБ	3	2,2	0,895
6	Политика ИБ	5	5,0	0,993
7	Управление доступом	4	3,6	0,973
8	Управление уязвимостями	3	2,2	0,895
9	Управление ЖЦ АС	4	3,6	0,973
10	Управление информационными активами	3	2,2	0,895
11	Управление изменениями	3	2,2	0,895
12	Архитектура ИБ	4	3,6	0,973
13	Управление каналами связи	4	3,6	0,973
14	Управление внешним взаимодействием	3	2,2	0,895
15	Разведка угроз ИБ	3	2,2	0,895
16	Управление событиями ИБ	4	3,6	0,973
17	Управление инцидентами ИБ	4	3,6	0,973
18	Антикризисное управление	3	2,2	0,895
19	Обеспечение непрерывности бизнеса	5	5,0	0,993
20	Повышение осведомленности персонала	3	2,2	0,895
21	Безопасность персонала	5	5,0	0,993

В результате оценка $C_э$ доверия к эффективности процессов информационной безопасности организации в соответствии с формулой (10) равна:

$$C_э = \sqrt[21]{\prod_{i=1}^{21} d_i} = \sqrt[21]{0,282} = 0,942 .$$

Таким образом, оценка доверия к ИБ организации определяется значением функции (11):

$$D_C = \sqrt{0,81 \cdot 0,942} = 0,874.$$

Б. Измерение качества модели оценки доверия и бекграунда. Согласно п.6. качество модели оценки доверия будем оценивать с точки зрения того, в какой мере экспертный метод и процедура его реализации обеспечивает объединение математических моделей и оценочных суждений экспертов с целью получения достоверного результата. При этом будем использовать шкалу Харрингтона.

Пусть $\xi_{M_k} = 0,85$, $\xi_{L_k} = 0,93$ и $\xi_{M_э} = 0,95$, $\xi_{L_э} = 0,93$ − оценки полезности экспертного метода и процедуры его реализации для получения достоверных оценок доверия C_k и $C_э$ соответственно. Тогда по формулам (12) и (13) получим следующие оценки:

$$P_k = \sqrt{0,85 \cdot 0,93} = 0,89 , P_э = \sqrt{0,95 \cdot 0,93} = 0,94 ,$$

$$D_P = \sqrt{0,89 \cdot 0,94} = 0,91 .$$

Оценку бекграунда лиц, проводивших оценку доверия к ИБ, также будем давать по шкале Харрингтона.

Пусть $\xi_{B_k} = 0,76$ и $\xi_{B_э} = 0,83$ − оценки бекграунда лиц, проводивших оценку доверия к корректности и эффективности. Тогда согласно (14) получим:

$$D_B = \sqrt{0,76 \cdot 0,83} = 0,79 .$$

В. Оценка знаний относительно угроз. Пусть $\xi_R = 81$ и $\xi_F = 90$ − оценки достоверности свидетельств знаний R и F согласно шкале Кента. Полагая в (4) $y_{\min} = 1$ и $y_{\max} = 99$ получим:

$$y_R^н = -2 + 7 \cdot (81-1)/(99-1) = 3,71 ,$$

$$y_F^н = -2 + 7 \cdot (90-1)/(99-1) = 4,92 .$$

Тогда желательности d_R и d_F, согласно (3), будут иметь следующие значения:

$$d_R = \exp(-\exp(-3,71)) = 0,98 ,$$

$$d_F = \exp(-\exp(-4,92)) = 0,99 .$$

И, наконец, по формуле (15) получим оценку полезности знаний относительно угроз:

$$D_Z = \sqrt{d_R \cdot d_F} = \sqrt{0,98 \cdot 0,99} = 0,98 ,$$

а по формуле (16) − степень уверенности, с которой в организации реализована политика безопасности:

$$D_U = \sqrt[4]{D_C \cdot D_P \cdot D_B \cdot D_Z} = \sqrt[4]{0,87 \cdot 0,91 \cdot 0,79 \cdot 0,985} = 0,87 .$$

Такую уверенность по шкале Харрингтона можно интерпретировать как "очень высокая".

8. Выводы. Предложена модель оценки информационной безопасности организации по критерию уверенности с которой в организации реализована политика безопасности. Рассмотрены факторы формирования уверенности и в качестве ее интегрального показателя предложена обобщенная функция Харрингтона. Оценка уверенности включает оценку доверия к информационной безопасности организации, качества модели оценки доверия и бекграунда лиц, проводивших такую оценку и оценку знаний относительно угроз. В целом рассмотренный подход может быть использован в качестве пилотажа для разработки соответствующих методик оценки ИБ организаций различных форм собственности. А рассмотренный пример со всей очевидностью демонстрирует его доступность.

ЛИТЕРАТУРА

[1]. ISO/IEC 27000:2009, Information security management systems. Overview and vocabulary. [Электронный ресурс]. Режим доступа: https://www.iso.org/standard/41933.html.

[2]. И. Чибрикин, "Информационная безопасность для организаций с высоким уровнем риска: новые угрозы и возможные подходы к их нейтрализации. Организационные и правовые аспекты информационной безопасности", *JetInfo №1, «ІІнфосистемы Джет»*, Москва, 2007.

[3]. И. Ажмухамедов, О. Князева, Л. Большакова, "Оценка уровня информационной безопасности финансовых учреждений", *Современные проблемы науки и образования*, № 1, 2015.

[4]. Ю. Шеховцова, "О субъективных аспектах понятия «безопасность»", *Экономика и современный менеджмент: теория и практика: сб. ст. по матер. V междунар. науч.-практ. конф.* Новосибирск: СибАК, 2011.

[5]. ISO/IEC TR 15443-1:2005 «Information technology. Security techniques. A framework for IT security assurance. Part 1: Overview and framework».

[6]. ISO/IEC 15408-1:2009 Information technology -- Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model.

[7]. ISO/IEC 21827:2008 Information technology. Security techniques. Systems Security Engineering. Capability Maturity Model® (SSE-CMM®).

[8]. П. Шиверов, В. Бондаренко, "Понятие доверия в контексте информационной безопасности", *ІІнформационные технологии и нанотехнологии.* СГАУ, Самара, С. 414-418, 2016.

[9]. Я. Имамвердиев, "Модель оценки доверия к информационной безопасности э-государства", *Проблемы информационных технологий. Институт ІІнформационных Технологий НАНА*, Баку, Азербайджан, №1, С. 25-32, 2015.

[10]. С. Зефиров, В. Голованов, "Как измерить информационную безопасность организации? Объективно о субъективном", *Защита информации, ІІнсайд.* Издательский Дом "Афина", Санкт-Петербург, № 3 (9), С. 28-35, 2006.

[11]. СТО БР ИББС–1.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». [Электронный ресурс]. Режим доступа: http://www.iso27000. ru/ standarty/ sto- br- ibbs- standarty-banka-rossii-v-oblasti-informacionnoi-bezopasnosti/st11.pdf/view

[12]. С. Скрыль, А. Курило, В. Финько, В. Чашкин, "Конфиденциальность как субъективный показатель защищенности информации", *Безопасность информационных технологий. «МІФІ» (НІЯУ МІФІ)*, Том 16, № 3, С. 141-144, 2009.

[13]. Ю. Шеховцова, "О субъективных аспектах понятия «безопасность»", *Экономика и современный менеджмент: теория и практика: сб. ст. по матер. V междунар. науч.-практ. конф.* Новосибирск: СибАК, 2011.

[14]. О. Зотова, "Научно-практические трактовки проблемы безопасности личности", *Прикладная юридическая психология*, №3. С. 128-132, 2010.

[15]. Canadian Tusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.

[16]. E. Harrington, The desirable function, Industrial Quality Control, vol. 21, no. 10, pp. 494-498, 1965.

[17]. G. Fechner, *Elemente der psychophysik, 2 Vols.* Leipzig (Germany): Breitkopf und Härtel, 1860, 571 p.

[18]. Ю. Чукова, Закон Вебера-Фехнера, М.: Гигиена, 2009, 144 с.

[19]. Ю. Самохвалов, О. Бурба, "Оценка эффективности научных и научно-технических проектов на основе обобщенной функции Харрингтона", *Системи управління, навігації та зв'язку*, вип.4(50), С. 77-85, 2018.

[20]. СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. [Электронный ресурс]. Режим доступа: http://www.garant.ru/products/ipo/prime/doc/ 70567254/.

[21]. Н. Милославская, Р. Сагиров, "Обзор моделей зрелости процессов управления информационной безопасностью", *Безопасность информационных технологий. МІФІ (НІЯУ МІФІ)*, Москва. Том 22, № 2, С. 76-84, 2015.

[22]. К. Нарыжный, Cobit 5: модель оценки процессов [Электронный ресурс]. Режим доступа: https://cleverics.ru/subject-field/articles/554-cobit5-pam.

[23]. Оценка зрелости процессов обеспечения информационной безопасности в российских банках [Электронный ресурс]. Режим доступа: https://www.pwc.ru/en/blogs/cybersecurity/posts/27ndpost.pf.
[24]. Ю. Самохвалов, Е. Науменко, *Экспертное оценивание*, ДУИКТ, К.: 2007, 268 с
[25]. Ю. Самохвалов, "Оценка обоснованности управленческих решений на основе нечеткой логики", *Управляющие системы и машины*, №3, 2017, С. 26-34.
[26]. S. Kent, *Strategic Intelligence for American World Policy,* Princeton: Princeton University Press, 1949, 226 p.
[27]. В. Плэтт, *Информационная работа стратегической разведки. Основные принципы*. Издательство иностранной литературы, Москва, 1958, 144 с.

ОЦІНКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ ЗА КРИТЕРІЄМ ВПЕВНЕНОСТІ

На даний час захист інформації залишається актуальною проблемою, а найбільш поширеними підходами до її оцінки є верифікаційний і ризик-орієнтований. Однак, метрики інформаційної безпеки (ІБ) у відповідних методиках, які засновані на цих підходах недостатньо інформативні, так як враховують лише об'єктивні аспекти безпеки, абсолютно ігноруючи суб'єктивні. Тому вони не дозволяють виробити основні судження про стан конфіденційності, цілісності та доступності інформації та рівні ІБ організації в цілому. У зв'язку з цим виникає необхідність в розробці методичного апарату оцінки ІБ організації з урахуванням об'єктивних і суб'єктивних аспектів безпеки. У статті пропонується підхід до оцінки ІБ на основі критерію впевненість в тому, що в організації реалізується прийнята політика безпеки. Оцінка впевненості включає оцінку довіри до інформаційної безпеки організації, якості моделі оцінки довіри і бекграунду осіб, які проводили таку оцінку і оцінку знань щодо загроз. У якості показника впевненості використовується показник корисності, як значення узагальненої функції бажаності Харрінгтона. Запропонований підхід до оцінки ІБ організації є досить простим в реалізації і може бути використаний в якості пілотажу для розробки відповідних методик оцінки ІБ організацій різних форм власності.
Ключові слова: оцінка, інформаційна безпека, впевненість, довіра, функція Харрінгтона, модель зрілості.

ASSESSMENT OF ORGANIZATION'S INFORMATION SECURITY ON THE CRITERION OF CONFIDENCE

Currently, the protection of information remains a pressing issue, and the most common approaches to its assessment are verification and risk-oriented method. However, the information security metrics in the relevant methodologies based on these approaches are insufficiently informative, since they take into account only objective aspects of security, completely ignoring the subjective ones. Therefore, they do not allow the development of judgments based on the state of confidentiality, integrity and availability of information and the organization's information security level as a whole. For that reason, there is a necessity to develop a methodological apparatus for assessing the organization's information security, taking into account objective and subjective aspects of security. The article proposes the approach to assessing information security on the basis of the criterion of confidence that an organization implements its adopted security policy. Assessment of confidence includes assessment of the credibility of organization's information security, the quality of the trust assessment model and the background of the persons who conducted such an assessment and knowledge assessment regarding threats. As an indicator of confidence, the utility indicator is used as the value of the generalized Harrington's desirability function. The proposed approach to assessing the organization's information security is fairly simple to be implemented and can be used as a pilot to develop appropriate methods for assessing the security of organizations of various forms of ownership.
Key words: assessment, information security, confidence, trust, Harrington's function, maturity model.

Самохвалов Юрий Яковлевич, доктор технических наук, профессор, профессор кафедры интеллектуальных и информационных систем Киевского национального университета имени Тараса Шевченко.
E-mail: yu1953@ukr.net.
Orcid ID: 0000-0001-5123-1288.
Самохвалов Юрій Якович, доктор технічних наук, професор кафедри інтелектуальних та інформаційних систем Київського національного університету імені Тараса Шевченка.
Samokhvalov Yuriy, Doctor of Engineering Science, Full Professor, professor of department of intellectual and informational systems of the Taras Shevchenko National University of Kyiv.

Браиловский Николай Николаевич, кандидат технических наук, доцент, доцент кафедры кибербезопасности и защиты информации Киевского национального университета имени Тараса Шевченко.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.
Браіловський Микола Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і захисту інформації Київського національного університету імені Тараса Шевченка.
Brailovskyi Mykola, PhD in Engineering Science, Associate Professor, Associate Professor of department of Cybersecurity and Information Protection of the Taras Shevchenko National University of Kyiv.