DOI 10.37882/2223-2966.2023.9-2.10

ХАРАКТЕРИСТИКА МЕТОДИК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАН ЕВРОСОЮЗА[1]

CHARACTERISTICS OF THE METHODS OF ENSURING INFORMATION SECURITY OF THE EU COUNTRIES

V. Elin
A. Tsaregorodtsev
M. Lavrinenko

Summary. The article reveals the centrally applied methods in the EU countries for ensuring information security of certain categories of restricted access information, based on the definition of criteria for the severity of a violation of the context, on a set of requirements to ensure effective and coordinated activities of certified Cybersecurity Assessments modules, as well as on the use of an interoperable set of risk management tools in the EU countries.

Keywords: information security, restricted access information, security methods, information threats, vulnerabilities of information systems.

Елин Владимир Михайлович
Кандидат педагогических наук, доцент, доцент, Финансовый университет при Правительстве Российской Федерации;
Кандидат педагогических наук, доцент, доцент, МОСУ МВД РФ им. В.Я. Кикотя
Царегородцев Анатолий Валерьевич
Доктор технических наук, профессор, Финансовый университет при Правительстве Российской Федерации
anvtsaregorodtsev@fa.ru
Лавриненко Михаил Михайлович
Кандидат технических наук, доцент, доцент, Финансовый университет при Правительстве Российской Федерации

Аннотация. В статье раскрываются централизовано применяемые в странах Евросоюза методики обеспечения информационной безопасности отдельных категорий информации ограниченного доступа, основанные на определении критериев серьезности нарушения контекста, на совокупности требований по обеспечению эффективной и согласованной деятельности сертифицированных модулей Cybersecurity Assessments, а также на применении интероперабельного набора инструментов управления рисками в странах Евросоюза.

Ключевые слова: информационная безопасность, информация ограниченного доступа, методы обеспечения безопасности, информационные угрозы, уязвимости информационных систем.

В настоящее время в нашей стране в целях повышения качественных характеристик борьбы с коррупционными правонарушениями[1] осуществляется активное применение современных информационных технологий, применение которых обеспечивает предупреждение, выявление, пресечение, раскрытие и расследование причин коррупции и коррупционных правонарушений.

В качестве информационно-коммуникационной технологии обеспечения профилактики коррупционных преступлений определена автоматизированная система обработки информации «Посейдон», реализующая информационно-аналитическое обеспечение аналитической и проверочной деятельности в целях противодействия коррупции[2] состав и источники информации, содержащейся в системе «Посейдон», определяются ее координатором совместно с оператором системы «Посейдон» с участием поставщиков информации. В состав информации могут входить персональные данные лиц.

Защита информации ограниченного доступа в системе «Посейдон», ее использование и предоставление осуществляются в соответствии с законодательством Российской Федерации. При этом Федеральный Закон «О противодействии коррупции»[3] связывает защиту информации с запретом для должностных лиц «разглашать или использовать в целях, не связанных с выполнением служебных обязанностей, сведения, отнесенные к информации ограниченного доступа, ставшие им известными в связи с выполнением служебных обязанностей».

[1] Федеральный Закон от 25.10.2008 г. № 273-ФЗ «О противодействии коррупции» // СЗ РФ, 29.12.2008, № 52 (ч. 1), ст. 6228.

[2] Указ Президента РФ от 25.04.2022 № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» (вместе с «Положением о государственной информационной системе в области противодействия коррупции «Посейдон»)//http://www.kremlin.ru/acts/bank/47769.

[3] Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» // СЗ РФ 2008. № 52 (Ч. 1). Ст. 6228.

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

В сложившихся условиях особый интерес представляет анализ зарубежного опыта по разработке и применению методологий обеспечения информационной безопасности отдельных категорий информации ограниченного доступа, некоторые из которых представлены в данной статье.

Методология оценки серьезности нарушений персональных данных[4] устанавливает критерии оценки для определения серьезности нарушения, к которым относит: контекст обработки данных (Data Processing Context (DPC), простоту идентификации (Ease of Identification (EI) и обстоятельства нарушения (Circumstances of breach (CB).

Окончательное значение серьезности нарушений рассчитывается по формуле:

$$SE = DPC*EI + CB \quad (1)$$

При этом показатели для параметров расчета определяются с учетом ряда табличных критериев:

В основе методологии оценки нарушений персональных данных положено применения критерия критичности данного набора данных DPC в конкретном контексте обработки. Результат относится к определенному диапазону значений, который соответствует одному из четырех уровней серьезности: низкий, средний, высокий и очень высокий. Контекст обработки данных (DPC) наряду с типом взломанных данных учитывает факторы контекста обработки. Предварительный балл DPC получаем в результате классификации персональных данных: простые, поведенческие, финансовые и конфиденциальные данные, затем параметр корректируется с учетом контекстуальных факторов, связанных с конкретным типом данных.

Простота идентификации (EI), представляет собой характеристику затратности установления личности физических лиц и определяет возможность соотнесения персональных данных с конкретным физическим лицом. Различают четыре уровня EI (незначительный, ограниченный, значительный и максимальный) с линейным увеличением баллов. Самый низкий балл присваивается, когда возможность идентифицировать личность ничтожно мала, поскольку сопоставить данные с конкретным человеком чрезвычайно сложно, но возможно при определенных условиях. Идентификация может быть прямой (например, на основе имени) или косвенной (например, на основе идентификационного номера), на основе взломанных данных, также может зависеть от конкретного контекста взлома, когда идентификация возможна непосредственно на основе взломанных данных без специальных исследований, необходимых для установления личности человека.

Обстоятельства нарушения (CB) представляют собой конкретные обстоятельства, связанные с типом нарушения, включая главным образом утрату безопасности взломанных данных с учетом таких элементов как потеря безопасности (конфиденциальность, целостность, доступность) и злонамеренный умысел, что позволяет дополнить DPC и EI.

Потеря конфиденциальности происходит при обращении к информации участников, которые либо не уполномочены, либо не имеют законного доступа. Степень потери конфиденциальности зависит от объема раскрытия, т.е. от потенциального количества и типа сторон, которые получили (могут получить) незаконный доступ к информации.

Потеря целостности происходит в случае изменения содержания исходной информации, что может нанести ущерб заинтересованному лицу. Наиболее серьезная ситуация возникает, когда существуют серьезные возможности того, что измененные данные были использованы таким образом, который мог нанести вред человеку.

Потеря доступности происходит, когда утрачивается возможность доступа к запрашиваемым исходным данным, что может носить временный (данные могут быть восстановлены, но это займет определенный период времени, и это может нанести ущерб человеку), либо постоянный (данные не могут быть восстановлены) характер.

Злонамеренность умысла следует связывать человеческой или технической ошибкой, либо с неправомерным воздействием. В случае ошибки нарушения включают случаи потери, ненадлежащего удаления, человеческой ошибки и программного сбоя или неправильной настройки. Неправомерные нарушения включают случаи кражи и взлома, направленные на причинение вреда отдельным лицам, а также передачу персональных данных третьим лицам с целью получения прибыли (например, продажу списков персональных данных).

Баллы, полученные за каждый элемент CB, суммируются.

Окончательная оценка представлена в табл. 1 и показывает уровень серьезности нарушения с учетом влияния на физических лиц.

Методология отраслевых оценок кибербезопасности[5] (Sectoral Cybersecurity Assessments Далее:

[4] Recommendations for a methodology of the assessment of severity of personal data breaches. Working Document, v1.0, December 2013/European Union Agency for Network and Information Security.

[5] Methodology for sectoral cybersecurity assessments.eu cybersecurity certification framework. Sept.2021/ENISA.142 P.S

«Методология SCSA») определяет совокупность требований по обеспечению эффективной и согласованной деятельности сертифицированных модулей Cybersecurity Assessments (CSA).

Таблица 1.

Уровень серьезности утечки данных

SE < 2	Низкий	Люди либо не будут затронуты, либо могут столкнуться с некоторыми неудобствами, которые они без проблем преодолеют (затраты на повторный ввод информации, досада, раздражение и т. д.).
2 ≤ SE < 3	Средний	Люди могут столкнуться со значительными неудобствами, которые они в состоянии преодолеть, несмотря на некоторые трудности (дополнительные расходы, отказ в доступе к бизнес-услугам, страх, непонимание, стресс, незначительные физические недуги и др.).
3 ≤ SE< 4	Высокий	Люди могут столкнуться со значительными последствиями, которые они в состоянии преодолеть, пусть и с серьезными трудностями (утрата финансовых средств, занесение в черный список банками, материальный ущерб, потеря работы, повестка в суд, ухудшение здоровья и др.).
4 ≤ SE	Очень высокий	Физические лица могут столкнуться со значительными, или необратимыми последствиями, которые они не могут преодолеть (существенный долг или неспособность работать, долгосрочные психологические или физические недуги, смерть и др.).

Выделяют следующие задачи: выполнение требований безопасности и гарантии услуг, процессов или продуктов ИКТ, определяемых на основе рисков, связанных с предполагаемым использованием ИКТ; обеспечение гарантированных уровней поддержки и применение инструментов встроенной безопасности. Решение представленных задач с помощью методологии SCSA осуществляется в контексте разработки отраслевых схем сертификации кибербезопасности для различных услуг ИКТ в отдельных секторах рынка.

Исследователи выделяют ряд особенностей методологии SCSA:

— основой оценки кибербезопасности на отраслевом уровне выступают цели функционирования ИКТ в отрасли, основные активы и связанные с ними риски, на основе анализа информации об использовании подсистем, продуктов или услуг. Важным параметром при анализе киберугроз (CTI), необходимым для определения требований безопасности и гарантии к подсистемам ИКТ, продуктам ИКТ или услугам ИКТ на основе риска, выступают сведения о потенциальных злоумышленниках, их мотивах и возможностях;

— применение методологии SCSA основывается на применении внутренних эталонных уровней риска, безопасности и надежности, позволяет интегрировать и подходы к обеспечению кибербезопасности по секторам, продуктам и процессам, в том числе и основанных на основании требований ISO/IEC 15408[6].

Методология SCSA формирует взаимосвязь между стандартами серий ISO/IEC 27000 и ISO/IEC 15408, обеспечивая:

— обмен результатами оценки рисков, спецификациями безопасности и гарантиями на основании метода сопоставления, устраняющего расхождения в терминологии и обеспечивающего передачу информации;

— применение масштабируемых средств контроля с заданным уровнем безопасности в соответствии со способностью анализа рисков и защиты от атак. При этом заинтересованные стороны несут ответственность за выявление рисков и участвуют в определении требований безопасности, что позволяет связать совокупность рисков и затрат для снижения этих рисков;

— применение методологии SCSA обеспечивает согласованность в реализации уровней доверия на основании типовых схем применения, что позволяет использовать различные сертификаты.

Методология предлагает участникам отдельные алгоритмы поведения, основанные на совокупности типичных обязанностей:

— координирующий орган определяет правила участия заинтересованных организаций в отраслевой системе ИКТ, включающие, например, сертификацию безопасности подсистем или продуктов ИКТ в качестве предварительного условия участия в информационной системе или ее эксплуатации;

— совокупность предоставляемых инфраструктурных услуг, продуктов и процессов ИКТ, возможность их повсеместного использования, уровень детализации функций и уровней безопасности, определяется координирующим органом;

— качество отраслевых систем основано на требованиях соглашений об оказании услуг, заключаемых между конечными пользователями отраслевых услуг ИКТ с «поставщиком услуг ИКТ» или «розничным продавцом услуг ИКТ».

[6] ГОСТ Р ИСО/МЭК 15408-1-2012 «Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model». Национальный Стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

Методология SCSA реализует подход сценария риска для обеспечения согласованности и обратимости соображений риска, потенциала атаки, безопасности и гарантии, которые соединяют все три уровня отраслевой оценки.

На первоначальном этапе вычисление отраслевой оценки базируется на информации о первичных функциональных активах бизнес-процессов, далее оценивается потенциальное влияние успешных атак на первичные активы и вероятность того, что это воздействие может произойти. Информация о рисках предоставляется отраслевыми заинтересованными сторонами или генерируется любым инструментом управления рисками в соответствии со стандартом ISO/IEC 27005[7] и используется для консолидации оценки воздействия и вероятности конкретного инцидента и дальнейшего присвоения классов мета-риска (MRC).

Классы мета-риска в дальнейшем распространяют на все вспомогательные активы и используют для определения требований безопасности для подсистем, продуктов, услуг и процессов ИКТ.

Информация о риске, в частности MRC, применяется к конкретному вспомогательному активу, наследуется от оценки первичной информации или функционального актива, поддерживаемого оцениваемым вспомогательным активом. Для отраслевой оценки на высоком уровне как часть контекста используют CTI и информацию о нарушителях с учетом их потенциала и мотивов, в результате чего формируют перечень потенциальных типов нарушителей, с указанием целей, мотивации, а также оценки используемых нарушителями средств.

Подход в организационной системе управления информационной безопасностью (ISMS) базируется на оценке уровня риска как функции воздействия (последствий) события и вероятности его возникновения, причем методология позволяет оценить ущерб в результате инцидента лишь при условии высокой вероятности события либо при низкой степени воздействия на ИКТ, в связи с чем для предлагаемая модель сертифицируется для каждого сектора экономики на основании сопоставимых уровней риска.

Оценки отраслевых рисков проводятся координирующим органом сектора или разработчиком отраслевой схемы сертификации кибербезопасности с привлечением заинтересованных сторон и координирующих организаций («владельцев бизнес-рисков»), а также потребителей отраслевых услуг.

[7] ГОСТ Р ИСО/МЭК 27005-2010 Национальный Стандарт Российской Федерации "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management.

Методология SCSA базируется на сценариях риска, разрабатываемых отраслевыми заинтересованными сторонами с учетом возможного причиняемого ущерба.

Идентификация сценариев основывается на средствах и мотивации нарушителей, а также на их возможности оказывать влияние на функциональные (основные или вспомогательные) активы. По результатам идентификации сценариев риска заинтересованные стороны производят оценку вероятности реализации сценария, причем сценарий риска может касаться целей нескольких заинтересованных сторон, и в то же время разные заинтересованные стороны в секторе могут по-разному относиться к соответствующему воздействию. В связи с этим Методология SCSA предлагает две концепции согласования решений, касающихся воздействия, которое может быть вызвано реализацией данного сценария риска.

В целях обеспечения сопоставимости оценок воздействия по секторам, определяются общие уровни воздействия для использования в оценках отраслевых рисков. Эти уровни, называемые классами воздействия (IC), качественно измеряют ущерб, который сценарий риска может нанести бизнесу заинтересованных сторон.

Инструменты управления рисками в Евросоюзе (Interoperable EU Risk Management Framework («EU RM»)

Интероперабельный набор инструментов EU RM[8] обеспечивает справочную структуру для интерпретации, сравнения и агрегирования результатов полученных с помощью различных методов оценки риска[9]. Это позволяет заинтересованным сторонам работать над общими угрозами и сценариями рисков[10] и сравнивать уровни рисков, даже в тех случаях, когда они оцениваются с помощью различных или собственных инструментов и методов, что позволяет разработать комплексное представление о состоянии кибербезопасности организаций в отношении конкретных или возникающих угроз в разных секторах и странах.

Функциональными компонентами набора инструментов EU RM являются следующие: отображение терминологии; сопоставление активов; картирование угроз и уровней риска. Набор инструментов EU RM облегчает согласование действий по четырем направлениям менеджмента рисков:

— предоставляет набор интероперабельных терминов, основанных на нормативно-правовой базе и международных стандартах, которые исполь-

[8] Interoperable EU Risk Management Toolbox. February. 2023.

[9] Сборник структур управления рисками с потенциальной функциональной совместимостью// https://www.enisa.europa.eu/publications/compendium-of-risk-management frameworks.

[10] Интероперабельная система управления рисками ЕС // https://www.enisa.europa.eu/publications/interoperable-eu-risk-management framework.

зуются для установления контекста RM. Это позволяет дать однозначное описание и понимание деятельности RM, осуществлять сопоставление между набором инструментов EU RM и соответствующими методологиями RM, независимо от используемой методологии RM;

— определяет объем среды применения оценки рисков, предоставляя классификацию основных и дополнительных активов участников. Классификация облегчает разработку однозначных сценариев риска и правильную интерпретацию соответствующих активов, подлежащих учету в процессе оценки риска, после чего организации смогут определить, применим ли сценарий риска или атаки и каким образом;

— позволяет определить сценарии риска, связанные с конкретной угрозой или группой угроз. При этом сценарии высокого уровня риска, связанные с конкретной угрозой или группой угроз должны быть сопоставлены со средой организации для надлежащей оценки. После того, как произошел выбор сценария риска для оценки, инструментарий EU RM может использовать таксономию угроз, предоставленную набором инструментов, и активы, связанные со сценарием риска, чтобы сопоставить его с соответствующим внутренним методом RM. Это позволяет организациям легко оценивать свои уровни риска и состояние безопасности своей организации для сценариев риска и приступать к нормализации рассчитанных результатов;

— сопоставление рассчитанных с использованием выбранного метода RM значений рисков с общей шкалой рисков, на основании чего оператор нормализует результаты на основе процесса сопоставления уровней риска, специально разработанного для каждого RM. В процессе сопоставления соотносят шкалу рисков выбранного внутреннего метода со шкалой рисков набора инструментов, предоставляя тем самым заинтересованным сторонам средства для использования общей эталонной шкалы оценки рисков.

В информационной системе защите подлежат основные и вспомогательные активы, персонал[11], коммуникации[12] и организационную инфраструктуру[13].

В число основных активов относят основные бизнес-процессы, услуги и функции, предоставляемые третьими лицами; компьютерные данные (информация) для обслуживания конкретных производственных процессов.

В перечень вспомогательных активов включено аппаратное обеспечение, устройства и оборудование[14], средства массовой информации, устройства Интернета вещей (IoT), устройства операционных технологий (OT), телекоммуникационные устройства, периферийные устройства и устройства хранения; программное обеспечение и приложения[15].

Категоризация активов осуществляется на основании адаптированных к потребностям инструментария требований стандартов ISO/IEC 27005:2018[16].

В качестве основных угроз определены: природные и промышленные угрозы, ошибки и непреднамеренные сбои, преднамеренные нападения и сервисные угрозы (облачные сервисы и сервисы, предоставляемые третьими лицами).

После определения категорий угроз каждая отдельная угроза связуется с категориями активов, на которые она может повлиять и с последствиями, которые это может вызвать с точки зрения конфиденциальности, целостности и доступности.

Уровень риска информационной безопасности определяется как показатель степени воздействия потенциального события и связывается с вероятностью возникновения угрозы и ее влиянием на активы организации. Обычно используют три типа методологий оценки рисков информационной безопасности: количественные, качественные и полуколичественные. Количественная оценка риска использует объективные (подлежащие количественной оценке) факты, качественная оценка риска устанавливает риск для отдельных категорий информации, метод полуколичественной оценки риска обычно использует описательные или числовые оценки.

Риск определяют, как произведение вероятности возникновения и влияния угрозы.

Вероятность возникновения угрозы представляет собой оценку вероятности того, что конкретная угроза

[11] Персонал осуществляющий бизнес-процессы и функции, поддержку пользователей, разработку и обслуживание программного обеспечения, поддержку оборудования, предоставление услуг и управление данными.

[12] Инженерные коммуникации, включая все соответствующие помещения, а также основные коммунальные услуги, предоставляемые внешними поставщиками, электроснабжение и водоснабжение.

[13] Организационная инфраструктура, политики, процедуры и вспомогательные услуги информационно-коммуникационных технологий (ИКТ) (например, телекоммуникации, сеть, облако, хостинг).

[14] В т.ч. .вычислительные и сетевые устройства.

[15] Включая системное программное обеспечение и операционные системы, встроенное программное обеспечение, промежуточное программное обеспечение, пакетное программное обеспечение и бизнес-приложения/приложения для конечных пользователей.

[16] В настоящее время актуальной версией ISO/IEC 27005:2018 выступает ISO/IEC 27005:2022 "Information security, cybersecurity and privacy protection — Guidance on managing information security risks".

может использовать конкретную уязвимость или совокупность уязвимостей. Методология EU RM использует уровни вероятности возникновения непреднамеренных угроз: ежедневная, ежемесячная, ежегодная, один раз в 10 лет и один раз в столетие. Инструментарий EU RM определяет пять дискретных уровней вероятности возникновения угрозы: очень высокий (угроза, скорее всего, материализуется, поскольку существуют связанные с ней уязвимости и отсутствуют адекватные меры безопасности), высокий (угроза может материализоваться, потому что существуют связанные уязвимости, которые можно использовать, и применяются неэффективные или устаревшие меры безопасности), умеренный (угроза потенциально может материализоваться, поскольку существуют уязвимости, которые можно использовать, и несмотря на то, что они были закрыты мерами безопасности), низкий (угроза вряд ли материализуется, так как все связанные с ней уязвимости закрыты соответствующими мерами безопасности), очень низкий (возникновение угрозы крайне маловероятно).

Уровень воздействия определяется как уровень ущерба, который может быть оценен в результате различных действий[17], Инструментарий EU RM определяет следующие пять уровней воздействия, описываемых с точки зрения операционных, правовых, финансовых и других последствий: очень высокий, высокий, умеренное, низкий, очень низкое.

Таким образом можно сделать вывод о том, что применяющиеся в странах Евросоюза методики обеспечения безопасности некоторых категорий информации ограниченного доступа базируется на применении критериев оценки контекста обработки данных, идентификации информации, характеристике угроз и вероятности наступления неблагоприятных последствий с учетом обстоятельств нарушения. К несомненным положительным чертам представленных методик относится их высокая вариативность и отсутствие жестких требований построения систем безопасности информационных систем обработки информации ограниченного доступа.

[17] Включая, помимо прочего, последствия незаконного раскрытия информации, незаконного изменения информации, несанкционированного уничтожения информации или потери информации, или доступности информационной системы.

ЛИТЕРАТУРА

1. Федеральный Закон от 25.10.2008 г. № 273-ФЗ «О противодействии коррупции» // СЗ РФ, 29.12.2008, № 52 (ч. 1), ст. 6228.
2. Указ Президента РФ от 25.04.2022 № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» (вместе с «Положением о государственной информационной системе в области противодействия коррупции «Посейдон»)//http://www.kremlin.ru/acts/bank/47769.
3. Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» // СЗ РФ 2008. № 52 (Ч. 1). Ст. 6228.
4. Recommendations for a methodology of the assessment of severity of personal data breaches. Working Document, v1.0, December 2013/European Union Agency for Network and Information Security.
5. Methodology for sectoral cybersecurity assessments.eu cybersecurity certification framework. Sept.2021/ENISA.142 P.S.
6. ГОСТ Р ИСО/МЭК 15408-1-2012 «Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model». Национальный Стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
7. ГОСТ Р ИСО\МЭК 27005-2010 Национальный Стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Information technology. Security techniques. Information security risk management.
8. Interoperable EU Risk Management Toolbox. February. 2023.
9. Сборник структур управления рисками с потенциальной функциональной совместимостью// https://www.enisa.europa.eu/publications/compendium-of-risk-management frameworks.
10. Интероперабельная система управления рисками ЕС // https://www.enisa.europa.eu/publications/interoperable-eu-risk-management framework.