DOI 10.52209/1609-1825_2025_2_364 УДК 004.056

Метод приоритезации рисков информационной безопасности для реагирования на инциденты информационной безопасности

[1]**АМРЕНОВ Асхат Казбекович,** *магистр, преподаватель, askhat.amrenov@gmail.com,*
[1]**НУРУШЕВА Асель Муратовна,** *PhD, и.о. ассоциированного профессора, nurusheva.assel@mail.ru,*
[1]***ТОКСЕИТ Динара Куандыккызы,** *PhD, старший преподаватель, tokseit1990@gmail.com,*
[2]**ГОРАНИН Николай,** *PhD, профессор, nikolaj-goranin@vilniustech.it,*
[1]НАО «Евразийский национальный университет имени Л.Н. Гумилева», ул. Сатпаева, 2, Астана, Казахстан,
[2]Вильнюсский технический университет имени Гедиминаса, аллея Саулетяке, 11, Вильнюс, Литва,
**автор-корреспондент.*

Аннотация. *В статье предлагается комбинированный метод управления рисками безопасности информационных систем, основанный на экспертных оценках и риск-ориентированных шаблонах. Оценки были получены путем проведения анкетирования (экспертная оценка), а также с помощью Common Vulnerability Scoring System (CVSS). CVSS использовалась для расчета уровня уязвимости и метрики вероятности угрозы после принятия контрмер. Этот метод может быть использован для определения приоритетности рисков информационной безопасности, а также для определения требований к информационной безопасности. Моделируются атаки на системы предотвращения утечек информации. Определены приоритеты рисков, связанных с этими атаками. Такие системы могут быть использованы в работе SOC и CERT. Таким образом, метод может быть использован на этапе построения бизнес-процессов, связанных с CSIRT.*

Ключевые слова: *информационная система, DLP, информационная безопасность, CSIRT, оценка рисков.*

Введение

Обеспечение информационной безопасности – важная задача в современном мире. Основными функциями команды CSIRT являются своевременное реагирование на инциденты информационной безопасности и их предотвращение, а также обнаружение уязвимостей в системе и оповещение об этих уязвимостях. Средства информационной безопасности помогают обнаруживать уязвимости, инциденты, происходящие в информационно-коммуникационной инфраструктуре предприятий. Данные средства также могут быть подвержены угрозам информационной безопасности, связанным с уязвимостями, а также групповыми атаками. Поэтому необходимо уметь оценивать и анализировать риски, связанные с этими угрозами и уязвимостями. В статье рассматриваются риски информационной безопасности, связанные с использованием средств предотвращения утечки данных (DLP).

Для исследования был проведен обзор литературы.

Об определении рисков, безопасности и надежности путем применения многокритериальных методов в различных практических сферах написано множество научных работ [1]-[3]. В работах [4]-[7] исследованы проблемы информационной безопасности и надежности, предложены методы обеспечения безопасности и надежности для идентификации и снижения рисков безопасности на начальном этапе построения ИС, а также построена подходящая программная система на основе предложенных методов.

В статьях [8]-[10] представлен новый подход к обеспечению информационной безопасности и надежности информационных и автоматизированных систем. Новый подход позволяет оценить безопасность и надежность компонентов ИС. Компоненты ИБ оцениваются по многим критериям с помощью методологии многокритериального принятия

решений, что позволяет достичь различных целей, связанных с обеспечением информационной безопасности и надежности ИБ.

Методы

Под сортировкой инцидентов информационной безопасности подразумевается процесс определения приоритета реагирования на инциденты ИБ в зависимости от степени воздействия на информационно-коммуникационную инфраструктуру, а также компрометации информационной системы. Команды реагирования на инциденты информационной безопасности сортируют уже случившиеся инциденты ИБ. В данной статье оценка производится частично экспертами и частично с помощью метода CVSS. Для описания системных задач, бизнес-процессов, уязвимостей, вероятных угроз и мер противодействия этим угрозам используется риск-ориентированная модель безопасности BPMN. Использование риск-ориентированной модели BPMN наглядно помогает выявлять, сортировать, оценивать риски. Метод может быть использован командами CSIRT перед подключением новых клиентов для выявления возможных уязвимостей, а также применяться для учета нюансов информационной безопасности при моделировании бизнес-процессов. Метод позволяет производить приоритезацию рисков информационной безопасности, равно как и определять требования к информационной безопасности. Преимуществами являются отсутствие необходимости в точных исходных данных, применение дорогих программных приложений, возможность оценить эффективность проекта, а также простота расчетов.

Согласно методу, сначала определяются активы организации, которые необходимо защитить, и критерии для определения уровня безопасности. Затем выявляются риски безопасности и предлагаются контрмеры по снижению рисков. После идентификации системных активов и бизнес-активов, выявления рисков безопасности и определения контрмер проводится опрос экспертов в форме анкетирования с целью оценки рисков безопасности. Полученные оценки позволяют провести дальнейший анализ и определить наиболее критичный риск информационной безопасности.

В данной статье рассматриваются 4 кейса, которые позволяют продемонстрировать применение метода по приоритезации рисков информационной безопасности для реагирования на инциденты информационной безопасности. Подробное описание приводится только для кейса 1.

Для кейса 1 бизнес-активы, системные активы и активы ИБ представлены на рисунке 1, где описан процесс авторизации администратора в DLP-системе. DLP-система обрабатывает имя пользователя и пароль, введенные пользователем. Если пароль и имя пользователя совпадают, то пользователю предоставляются привилегии администратора и присваивается определенный идентификатор сессии.

Риск информационной безопасности в этом случае может возникнуть в результате неправильного управления сеансами. Злоумышленник может использовать эту уязвимость для получения привилегий администратора DLP-системы с целью дальнейшего получения доступа к конфиденциальным документам. Благодаря уязвимости в DLP-системе злоумышленник может использовать атаку грубой силы для подбора идентификатора сессии и действовать от имени администратора.

В качестве контрмер для описанного выше риска предлагается реализовать «таймаут бездействия» для каждой сессии, для того чтобы сессия на сервере завершалась, когда пользователь выходит из системы.

Далее приводится описание контекста и модели активов, рисков и принятия контрмер для других трех случаев.

Описание контекста и модели активов для кейса 2, 3 и 4.

Для кейса 2 в качестве контекста модели и активов рассматривается процесс отправки клиентом dlp на сервер dlp уведомления о событии информационной безопасности. Информация о событии обрабатывается и отправляется в базу данных. Далее система формирует отчет и отправляет его на консоль администратора.

Для кейса 3 рассматривается процесс ввода данных администратором в подсистему DLP, отвечающую за управление событиями. Полученные данные подтверждаются информационной системой и принимаются для дальнейшей работы администратором DLP, который может просматривать события и кейсы на своей консоли с учетом обновленной информации.

Для кейса 4 рассматривается процесс регистрации нового пользователя DLP-системы. При регистрации новый пользователь отправляет DLP-системе свое имя пользователя и пароль. Пароль и логин подтверждаются DLP-системой и отправляются в базу данных.

Описание модели риска для кейсов 2, 3 и 4.

В качестве риска для второго кейса рассматривается уязвимость SQL-инъекции, которая может быть использована злоумышленником для удаленного выполнения кода на сервере и получения привилегий администратора для дальнейшего получения досту-

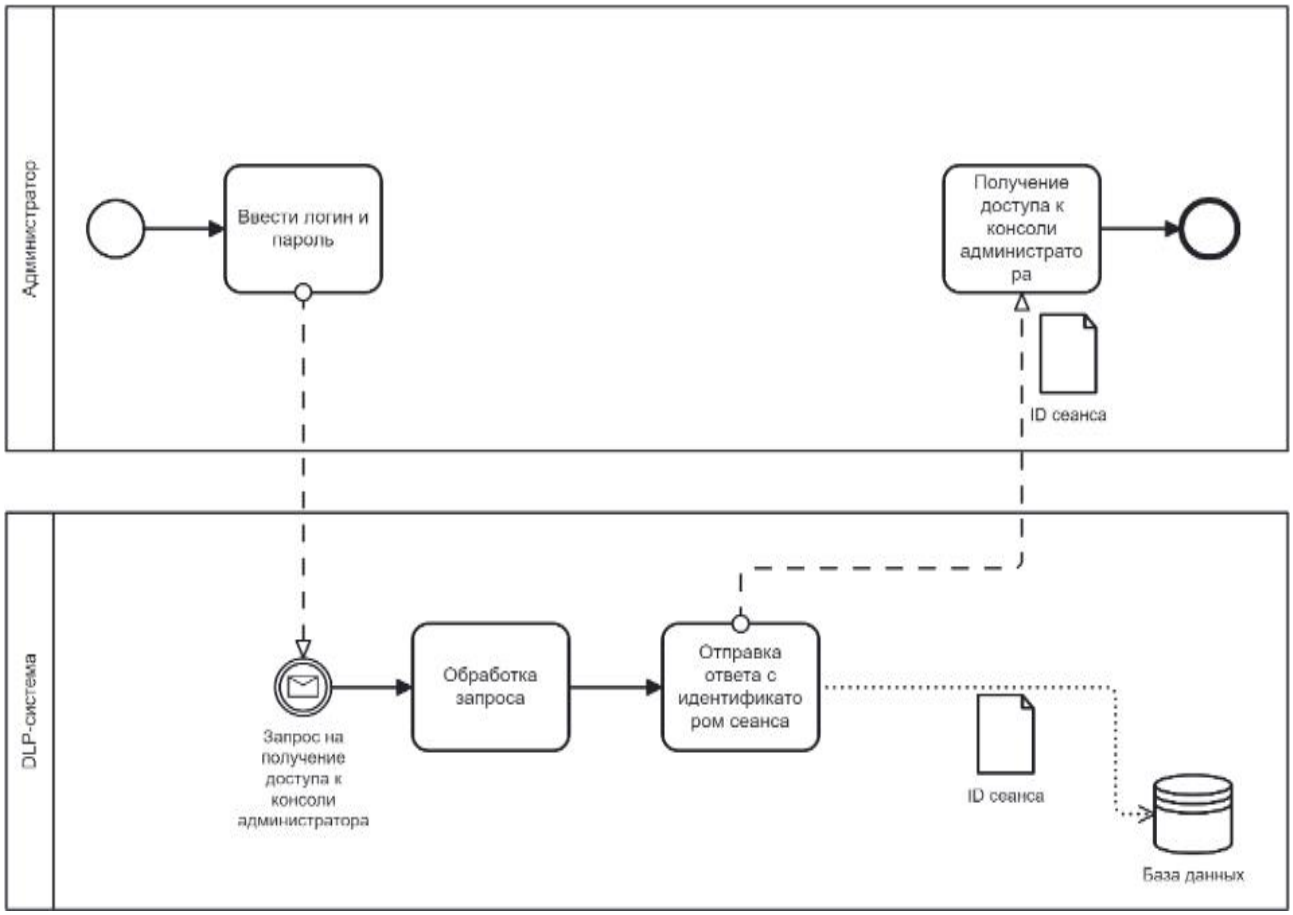


Рисунок 1 – Модель контекста и активов в риск-ориентированном BPMN

па к данным.

Для кейса 3 риском является уязвимость, благодаря которой злоумышленник внедряет вредоносную ссылку с помощью XSS-инъекции во фреймворк управления кейсами DLP.

В качестве риска для кейса 4 рассматривается уязвимость незащищенного хранения учетных данных. Данная уязвимость может позволить злоумышленнику прочитать данные, которые хранятся в базе данных, и таким образом получить доступ ко всем учетным данным.

Описание модели контрмер для кейсов 2, 3 и 4.

Для кейса 2 предлагается реализовать проверку вводимых данных и использовать параметризованные запросы.

Для кейса 3 предлагается реализовать проверку и фильтрацию вводимых данных.

Для кейса 4 предлагается рассмотреть возможность хранения криптографических хэшей паролей в качестве.

Далее, после идентификации всех моделей активов, рисков и контрмер происходит процесс оценки и анализа рисков.

Для того чтобы оценить риски информационной безопасности экспертным методом проводится анкетирование с целью ознакомить экспертов с риск-ориентированными моделями и получить оценки по таким метрикам, как стоимость контрмер, потребность в безопасности, ценность актива, уровень уязвимости и вероятность угрозы.

С помощью экспертов были получены оценки семи метрик. Также две другие оценки метрик были получены при помощи CVSS фреймворка. Оценки остальных метрик были посчитаны на основе ранее оцененных метрик.

Метрику ценности активов было предложено оценивать по шкале от 1 до 5. Метрику потребности в безопасности предлагалось оценивать по шкале от 1 до 3. Метрику уровня уязвимости предлагалось оценивать по шкале от 1 до 10. Метрику вероятности угрозы предлагалось оценивать по шкале от 1 до 10. Метрику стоимости контрмер предлагалось оценивать по шкале от 1 до 5.

Метрика потенциальной возможности события рассчитывалась как вероятность угрозы плюс уровень уязвимости минус один.

Метрика уровня воздействия рассчитывалась как максимальное значение метрики потребности в безопасности.

Метрика уровня риска рассчитывалась как потенциальная возможность события, умноженная на уровень воздействия.

Метрика уровня снижения риска рассчитывается как уровень риска 1 (уровень риска до принятия контрмер) – уровень риска 2 (уровень риска после принятия контрмер). Для расчета и оценки метрики уровня уязвимости и метрики вероятности угрозы после принятия контрмер использовалась общая система оценки уязвимостей (CVSS). Таким образом, метод оценки является комбинированным и состоит из двух методов – экспертного и CVSS. Комбинация этих методов с точки зрения экономии времени и повышения эффективности значительно упрощает и делает оценку рисков информационной безопасности более точной.

Для комбинированного метода оценки рисков безопасности были использованы Base score метрика и Exploitability subscore метрика из фреймворка CVSS.

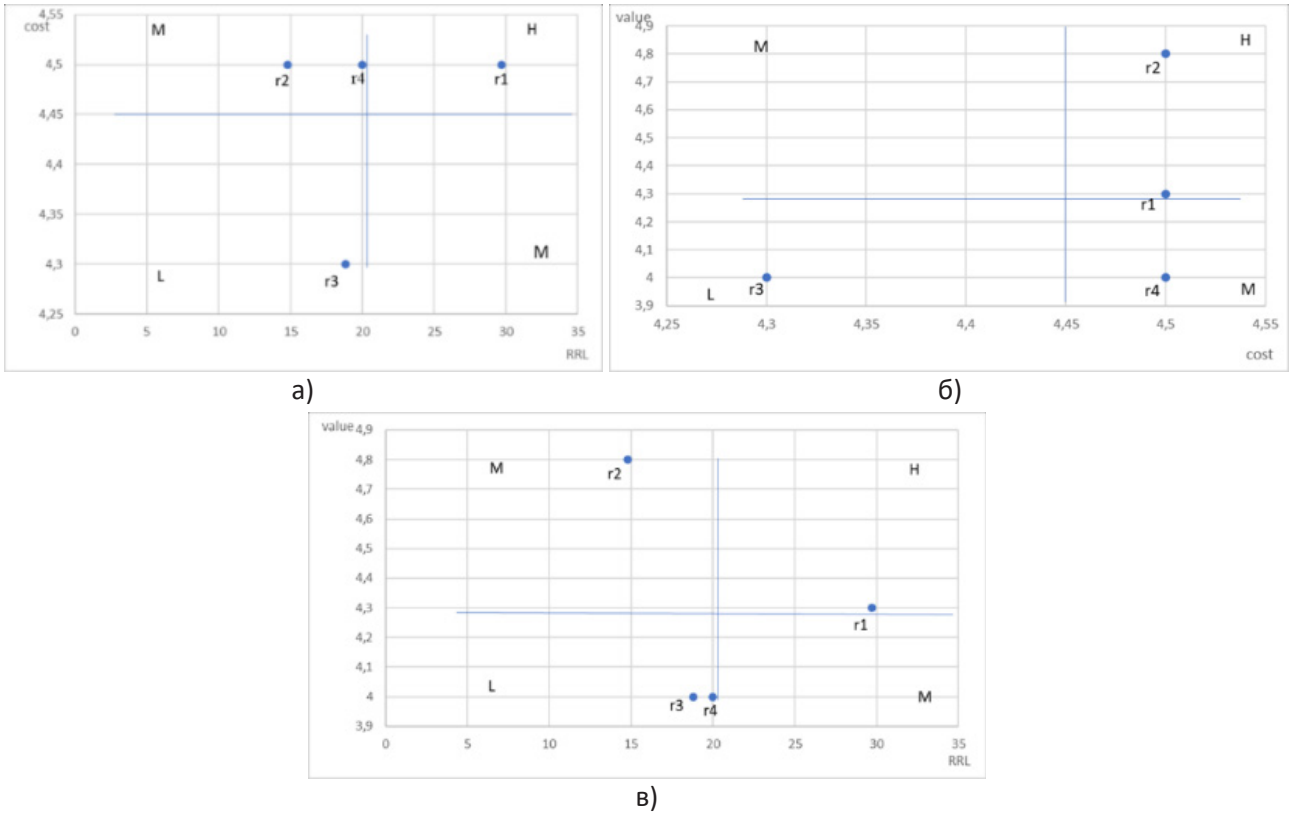
Результаты

На основе полученных данных был проведен анализ для выявления риска с наивысшим приоритетом. На рисунке 2 показана зависимость стоимости контрмер (cost) от уровня снижения риска (RRL), ценности актива (value) от стоимости и ценности актива от уровня снижения риска. Разделив каждую область рисунка на квадраты, можно определить приоритетность рисков. В данном случае для рисков 1, 2, 3 и 4 были такие оценки, как M (средний приоритет), L (низкий приоритет) и H (высокий приоритет). Для каждого риска был установлен приоритет.

Затем, в соответствии с диаграммами был подсчитан общий балл для каждого риска. Если риск попадает в область H, то начисляется 3 балла, если в область M, то 2 балла, если в область L, то 1 балл. Таким образом, риск суммарный балл которого является наибольшим, будет обладать наивысшим приоритетом. Риск, суммарный балл которого является наименьшим, будет обладать наименьшим приоритетом.

Обсуждение

В соответствии с определенными приоритетами рисков команда реагирования на инциденты информационной безопасности может определить, в какой последовательности реагировать на инцидент информаци-



а) б)

в)

Рисунок 2 – а) зависимость cost от RRL б) зависимость value от cost в) зависимость value от RRL

онной безопасности в случае осуществления инцидента ИБ, связанного с данными рисками, и затем предпринять необходимые действия и меры для устранения или минимизации риска. Если в SIEM-системе команды SOC или CSIRT вышло уведомление об обнаружении нескольких инцидентов информационной безопасности, то сначала рассматривается инцидент информационной безопасности, относящийся к риску с высоким приоритетом, затем рассматривают инциденты информационной безопасности связанные с рисками, имеющими средний приоритет, и в самую последнюю очередь рассматривают инциденты ИБ, связанные с рисками с низким приоритетом. Результаты показывают, что риск 1(r1) имеет наибольший приоритет. Следовательно, инцидент информационной безопасности, связанный с риском 1(r1) из кейса 1, будет обрабатываться первым. Исходя из полученных результатов следующие на очереди по реагированию будут инциденты информационной безопасности, относящиеся к риску 2 из кейса 2 и к риску 4 из кейса 4. Эти риски обладают средним приоритетом. Последним на очереди у команд CSIRT и SOC по реагированию будет инцидент, связанный с риском 3 из кейса 3 – XSS атака на компонент DLP-системы, отвечающий за управление событиями ИБ.

Заключение

В данной статье предложен комбинированный метод управления рисками безопасности информационных систем, основанный на экспертных оценках. Данные методы могут быть использованы для приоритезации рисков информационной безопасности на этапе сортировки инцидентов ИБ, а также для определения требований информационной безопасности при моделировании процессов информационной системы. Под сортировкой в контексте информационной безопасности понимается процесс определения приоритетности разрешения инцидентов в зависимости от степени серьезности нарушения или компрометации системы безопасности. По сути, команды реагирования сортируют уже произошедшие инциденты. В данной статье предлагается метод, основанный на экспертных оценках с использованием риск-ориентированных шаблонов для управления рисками безопасности информационных систем. Риск-ориентированные шаблоны информационной безопасности – это лучший способ в понятной и простой форме донести необходимую информацию, например, о технических аспектах информационной системы, до всех заинтересованных лиц, так или иначе связанных с этой информационной системой. Использование данного метода может наглядно помочь выявить, отсортировать, оценить риски и расставить приоритеты уязвимостей без применения технических средств. Предложенный метод рассматривается при моделировании атак на системы информационной безопасности от утечек. Определены приоритеты рисков, связанных с этими атаками. Такие системы могут быть использованы в работе SOC и CERT. Таким образом, метод может быть использован на этапе построения бизнес-процессов, связанных с SOC и CERT.

СПИСОК ЛИТЕРАТУРЫ

1. A. Abdiraman, N. Goranin, S. Balevicius, A. Nurusheva, I. Tumasonienė, "Application of Multicriteria Methods for Improvement of Information Security Metrics", Sustainability, vol. 15, no. 10:8114, 2023, doi:10.3390/su15108114.
2. T. Aidynov, N. Goranin, D. Satybaldina, A. Nurusheva, "A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography", Appl. Sci., vol. 14, no. 7:2742, 2024, doi: 10.3390/app14072742.
3. A. Boranbayev, S. Boranbayev, K. Yersakhanov, A. Nurusheva, R. Taberkhan, "Methods of Ensuring the Reliability and Fault Tolerance of Information Systems" in Adv. Intell. Syst. Comput.: 15th Int. Conf. Information Technology, 2018, pp. 729-730, doi: 10.1007/978-3-319-77028-4_93.
4. A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, "The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan" in Adv. Intell. Syst. Comput.: 15th Int. Conf. Information Technology, 2018, pp. 33-38, doi: 10.1007/978-3-319-77028-4_6.
5. A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, "Development of a Software System to Ensure the Reliability and Fault Tolerance in Information Systems", J. of Eng. Appl. Sci., vol. 13, no. 23, pp.

10080-10085, 2018, doi: 10.3923/jeasci.2018.10080.10085.
6. S. Boranbayev, N. Goranin, A. Nurusheva, "The methods and technologies of reliability and security of information systems and information and communication infrastructures", J. Theor. Appl. Inf. Technol., vol. 96, no. 18, pp. 6172-6188, 2018, doi: 2-s2.0-85055253568.
7. A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, Y. Seitkulov, "Development of web application for detection and mitigation of risks of information and automated systems", Euras. J. Math. Comp. Applic., vol. 7, no. 1, pp. 4-22, 2019, doi: 10.32523/2306-6172-2019-7-1-4-22.
8. Z. Turskis, N. Goranin, A. Nurusheva, S. Boranbayev, "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach", Inform., vol. 30, no. 1, 2019, pp. 265-289, doi: 10.15388/Informatica.2018.203.
9. S. Boranbayev, A. Amrenov, A. Nurusheva, A. Boranbayev, N. Goranin, Methods and Techniques of Information Security Risk Management During Assessment of Information Systems, in Adv. Intell. Syst. Comput. – Proc. of the 2022 Future of Inform. and Commun. Conf. (FICC), 2022, pp. 787-797, doi: 10.1007/978-3-030-98015-3_53.
10. Z. Turskis, N. Goranin, A. Nurusheva, S. Boranbayev, "A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development", Sustainability, vol. 11, no. 2:424, 2019, doi: 10.3390/su11020424.

Ақпараттық қауіпсіздік оқиғаларына жауап қайтару мақсатында қауіпсіздік тәуекелдерін приоритеттеу әдісі

[1]АМРЕНОВ Асхат Казбекович, *магистр, оқытушы, askhat.amrenov@gmail.com,*
[1]НУРУШЕВА Асель Муратовна, *PhD, қауымдастырылған профессор м.а., nurusheva.assel@mail.ru,*
[1]*ТОҚСЕИТ Динара Қуандыққызы, *PhD, аға оқытушы, tokseit1990@gmail.com,*
[2]ГОРАНИН Николай, *PhD, профессор, nikolaj-goranin@vilniustech.it,*
[1]«Л.Н. Гумилев атындағы Еуразия ұлттық университеті» КеАҚ, Сәтбаев көшесі, 2, Астана, Қазақстан,
[2]Гедиминас атындағы Вильнюс техникалық университеті, Саулетяке аллеясы, 11, Вильнюс, Литва,
**автор-корреспондент.*

Аңдатпа. *Ақпараттық жүйелер қауіпсіздігін басқарудың біріктірілген әдісі ұсынылған, ол сараптамалық бағалаулар мен тәуекелге бағытталған үлгілерге негізделген. Бағалар сауалнама (сараптамалық бағалау) және Common Vulnerability Scoring System (CVSS) арқылы алынды. CVSS қарсы шараларын қабылдағаннан кейін осалдық деңгейі мен қауіптің ықтималдық метрикасын есептеу үшін қолданылды. Бұл әдіс ақпараттық қауіпсіздік тәуекелдеріне басымдық беру, сондай-ақ ақпараттық қауіпсіздік талаптарын анықтау үшін пайдаланылуы мүмкін. Ақпараттың сыртқа шығуын болдырмау жүйелеріне жасалған шабуылдар модельденді. Осы шабуылдарға байланысты тәуекелдердің басымдықтары айқындалды. Мұндай жүйелер SOC және CERT жұмысында қолданылуы мүмкін. Осылайша, әдіс SOC және CERT-ке қатысты бизнес-процестерді құру кезеңінде пайдаланылуы мүмкін.*

Кілт сөздер: *ақпараттық жүйе, DLP, ақпараттық қауіпсіздік, CERT, тәуекелдерді бағалау.*

Method for Prioritizing Information Security Risks for Responding to Information Security Incidents

[1]AMRENOV Askhat, *Master's Degree, Teacher, askhat.amrenov@gmail.com,*
[1]NURUSHEVA Asel, *PhD, Acting Assistant Professor, nurusheva.assel@mail.ru,*
[1]*TOKSEIT Dinara, *PhD, Senior Lecturer, tokseit1990@gmail.com,*

*[2]**GORANIN Nikolaj,** PhD, Professor, nikolaj-goranin@vilniustech.it,*
[1]NPJSC «L.N. Gumilyov Eurasian National University», Satpayev Street, 2, Astana, Kazakhstan,
[2]Vilnius Gediminas Technical University, Sauletekio Alley, 11, Vilnius, Lithuania,
**corresponding author.*

***Abstract.** The article proposes a combined method for information system security risk management based on expert assessments and risk-based templates. The assessments were obtained by conducting questionnaires (expert judgment) and by using Common Vulnerability Scoring System (CVSS). CVSS was used to calculate the vulnerability level and a metric for the probability of threat after countermeasures. This method can be used to prioritize information security risks as well as to determine information security requirements. Attacks on information leakage prevention systems are modeled. The risks associated with these attacks are prioritized. Such systems can be used in SOC and CERT operations. Thus, the method can be used at the stage of building business processes related to SOC and CERT.*

***Keywords:** information system, DLP, information security, CERT, risk assessment.*

REFERENCES

1. A. Abdiraman, N. Goranin, S. Balevicius, A. Nurusheva, I. Tumasonienė, "Application of Multicriteria Methods for Improvement of Information Security Metrics", Sustainability, vol. 15, no. 10:8114, 2023, doi:10.3390/su15108114.
2. T. Aidynov, N. Goranin, D. Satybaldina, A. Nurusheva, "A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography", Appl. Sci., vol. 14, no. 7:2742, 2024, doi: 10.3390/app14072742.
3. A. Boranbayev, S. Boranbayev, K. Yersakhanov, A. Nurusheva, R. Taberkhan, "Methods of Ensuring the Reliability and Fault Tolerance of Information Systems" in Adv. Intell. Syst. Comput.: 15th Int. Conf. Information Technology, 2018, pp. 729-730, doi: 10.1007/978-3-319-77028-4_93.
4. A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, "The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan" in Adv. Intell. Syst. Comput.: 15th Int. Conf. Information Technology, 2018, pp. 33-38, doi: 10.1007/978-3-319-77028-4_6.
5. A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, "Development of a Software System to Ensure the Reliability and Fault Tolerance in Information Systems", J. of Eng. Appl. Sci., vol. 13, no. 23, pp. 10080-10085, 2018, doi: 10.3923/jeasci.2018.10080.10085.
6. S. Boranbayev, N. Goranin, A. Nurusheva, "The methods and technologies of reliability and security of information systems and information and communication infrastructures", J. Theor. Appl. Inf. Technol., vol. 96, no. 18, pp. 6172-6188, 2018, doi: 2-s2.0-85055253568.
7. A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, Y. Seitkulov, "Development of web application for detection and mitigation of risks of information and automated systems", Euras. J. Math. Comp. Applic., vol. 7, no. 1, pp. 4-22, 2019, doi: 10.32523/2306-6172-2019-7-1-4-22.
8. Z. Turskis, N. Goranin, A. Nurusheva, S. Boranbayev, "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach", Inform., vol. 30, no. 1, 2019, pp. 265-289, doi: 10.15388/Informatica.2018.203.
9. S. Boranbayev, A. Amrenov, A. Nurusheva, A. Boranbayev, N. Goranin, Methods and Techniques of Information Security Risk Management During Assessment of Information Systems, in Adv. Intell. Syst. Comput. – Proc. of the 2022 Future of Inform. and Commun. Conf. (FICC), 2022, pp. 787-797, doi: 10.1007/978-3-030-98015-3_53.
10. Z. Turskis, N. Goranin, A. Nurusheva, S. Boranbayev, "A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development", Sustainability, vol. 11, no. 2:424, 2019, doi: 10.3390/su11020424.