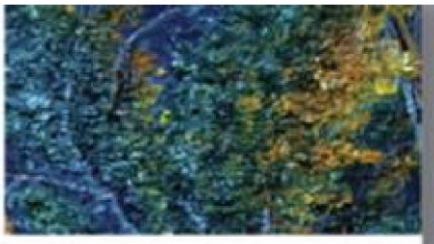

INTERNATIONAL SCIENCE REVIEWS

AIU

№3 (3) 2022

Natural Sciences and Technologies series

www.aiu.kz

ISSN: 2707-4862

ASTANA INTERNATIONAL UNIVERSITY

INTERNATIONAL SCIENCE REVIEWS
Natural Sciences and Technologies series

Has been published since 2020

№3 (3) 2022

Nur-Sultan
EDITOR-IN-CHIEF:

Doctor of Physical and Mathematical Sciences, Academician of NAS RK, Professor
Kalimoldayev M. N.

DEPUTY EDITOR-IN-CHIEF:

Doctor of Biological Sciences, Professor
Myrzagaliyeva A. B.

EDITORIAL BOARD:

Akiyanova F. Zh. - Doctor of Geographical Sciences, Professor (Kazakhstan)
Seitkan A. - PhD, (Kazakhstan)
Baysholanov S. S - Candidate of Geographical Sciences, Associate professor (Kazakhstan)
Zayadan B. K. - Doctor of Biological Sciences, Professor (Kazakhstan)
Salnikov V. G. - Doctor of Geographical Sciences, Professor (Kazakhstan)
Zhukabayeva T. K. - PhD, (Kazakhstan)
Urmashev B.A - Candidate of Physical and Mathematical Sciences, (Kazakhstan)
Abdildayeva A. A. - PhD, (Kazakhstan)
Chlachula J. - Professor, Adam Mickiewicz University (Poland) **Redfern S.A.T.** - PhD, Professor, (Singapore)
Cheryomushkina V.A. - Doctor of Biological Sciences, Professor (Russia)
Bazarnova N. G. - Doctor Chemical Sciences, Professor (Russia)
Mohamed Othman - Dr. Professor (Malaysia)
Sherzod Turaev - Dr. Associate Professor (United Arab Emirates)

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz

CONTENT

С.Е. Базаров СОВРЕМЕННОЕ СОСТОЯНИЕ УРОЖАЙНОСТИ МОЛОДИ ОКУНЯ И ПЛОТВЫ В ВЕРХНЕ-ЕРТИССКОМ КАСКАДЕ ВОДОХРАНИЛИЩ ……..…..…5

Д.Е. Ержанов ӨСКЕМЕН СУ ҚОЙМАСЫНЫҢ КӘСІПШІЛІК МАҢЫЗЫ БАР БАЛЫҚ ТҮРЛЕРІНІҢ ЭКОЛОГИЯЛЫҚБИОЛОГИЯЛЫҚ СИПАТТАМАСЫ ……..…..…11

С. Оңталапұлы, Н. Тасболатұлы МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ……..……..……..……21

А. Кусаинов STEM В КАЗАХСТАНЕ. ВИРТУАЛЬНАЯ РОБОТОТЕХНИКА В ШКОЛАХ ……..…….29

А.С. Муканова, А.Б. Барлыбаев, А.Е. Назырова, Л.Т. Кусепова РАЗРАБОТКА ОНТОЛОГИЧЕСКОЙ МОДЕЛИ ИЗБИРАТЕЛЬНОЙ СИСТЕМЫ.....34

М.Ж.Калдарова, А.Н.Султангазиева МЕТОДЫ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ ……..43

Ә.Ерланұлы, Е.М.Марденов, АНАЛИЗ ПРЕИМУЩЕСТВ И НЕДОСТАТКОВ VUE И REACT ……..……..53

МРНТИ 81.93.29

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

С. Оңталапұлы, Н. Тасболатұлы

Международный университет Астана,
Астана, Казахстан
E-mail: ontalapuly-s@mail.ru

Аннотация. Информационная безопасность и защищенность информации является актуальной областью, имеющей всестороннюю междисциплинарную связь. В данной статье рассматривается модели и методы оценки защищенности информации, освещаются проблемы безопасности и описываются средства контроля безопасности, рассматриваются шаги, включающее в себя сбор данных, критерии измерения воздействия рисков, определение проблемной области, относительная оценка угрозы и оценивание, определяющее выполнение требований в рамках кибербезопасности, так как все организации хранят множество данных, которые содержат информацию о производимых продуктах, о бизнес-процессах и о клиентах, соответственно возникает необходимость защищать и обеспечивать безопасность данных. Цель данного исследования состоит в изучении подходов для оценки защищенности информации и управлению информационной безопасностью. Анализируя защищенность информации самыми главными аспектами считаются выявление угроз и атак на системы компании. Соответственно у организациях возрастает необходимость проведения оценки систем безопасности и их соответствие требованиям, минимизировать уровень риска, тем самым обеспечивать непрерывность производства.

Ключевые слова: информационная безопасность, защищенность информации, угроза, уязвимость.

ВВЕДЕНИЕ

В нынешнее время обеспечение безопасности информации является самым актуальным вопросом, который включает в себя такие аспекты, как: безопасность программного обеспечения, компьютеров, электронных устройств, информационных систем, локальной инфраструктуры и многого другого и должен обеспечивать конфиденциальность информации, их целостность, а также доступность. Можно утверждать, что все организации хранят множество данных,

которые содержат информацию о производимых продуктах, о бизнес-процессах и о клиентах. Нарушение информационной безопасности могут привести к различным видам потерь и к негативным последствиям, получению несанкционированного доступа, злонамеренному повреждению цифровых активов компаний, а также могут повлиять на бизнес-деятельность фирмы, на деловые операции организации и на товары, производимые ей.

В работе [1] средства контроля защиты информации подразделяют на следующие три категории: технический контроль, формальный и неформальный контроль. Технические средства контроля осуществляют поддержку брандмауэров, криптографии и виртуальных частных сетей. Тем не менее они должны иметь формальные средства контроля, которые охватывают административные процедуры, предназначенные для предотвращения инцидентов, нарушений информационной безопасности (ИБ) и осуществления политики ИБ. А неформальные средства контроля сосредоточены на повышении осведомленности сотрудников об информационной безопасности посредством тренингов и программ обучения.

На многие компании злоумышленниками осуществляется вид атаки с использованием социальной инженерии для раскрытия конфиденциальной информации посредством психологического манипулирования сотрудников компании с целью совершения каких-либо действий. Например, открытие электронных документов, загрузка какого-либо файла, запуск программы, переход по ссылке и т.п. Также из множеств источников в интернете можно загрузить какие-либо вредоносные программы и запустить его в своей системе, которые потом невозможно детектировать антивирусной системой. Также посредством широко используемых программных обеспечений можно внедрить вредоносное программное обеспечение в операционную систему и запустить его. Примером этого является широко используемый офисный пакет Microsoft Office. Документы, созданные Microsoft Office содержат динамические элементы, предлагающее

расширенные функциональные возможности, привлекают интерес у злоумышленников. А динамические свойства элементов усиливаются с использованием языка программирования VBA. По данным Avira (2020) и Eset (2020) документы Microsoft Office является вторым, широко используемым форматом файлов вредоносными программами и применяется для рассылки спама.

В отчетах по кибербезопасности освещаются повторяющиеся проблемы безопасности, потеря данных, целевые атаки, различные уязвимости систем, приложений и устройств, кража и повреждение различной информации, похищение или уничтожение активов и т.п. Соответственно в организациях существуют множество уязвимостей, которые в будущем могут спровоцировать информационные угрозы, тем самым возникает необходимость производить аудит информационной безопасности, настраивать контроль доступа и повысить квалификации персонала по информационной безопасности. Вместе с изменением среды угроз атаки и инструменты для обеспечения безопасности динамично меняются. Обеспечение безопасности системы и защита конфиденциальности является самой актуальной проблематикой во всем мире. В связи с этим в данной статье будут отражены вопросы защиты информации и обеспечения безопасности информационной системы.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Основная цель исследования является оценка процесса управления информационной безопасностью и повышение уровня безопасности информации. Оценка процесса управления иформационной безопасностью с использованием эмпирических исследований требовало выполнения научно-обоснованных критериев оценки.

Для достижения поставленной цели необходимо произвести реализацию следующих теоретических по характеристике, задач:

- определение информационной безопасности в учреждениях;
- выявление угроз информационной безопасности в организациях;
- определение условий реализации системы управления информационной безопасностью.

Чтобы выполнить точный анализ защищенности информации, необходимо установить строгую методологию по управлению информационной безопасности, которые необходимо выполнить и затем оценить ожидаемые результаты каждого шага. Методология состоит из основных этапов, которые будут рассмотрены ниже.

1. **Сбор данных**. На данном этапе были собраны и проанализированы материалы по информационной безопасности и защиты информации из общедоступных источников, были проведены анализ модели, отраженные в этих работах и исследованы активы организации.

По итогу рассмотренных материалов, загруженных из базы Scopus были рассмотрены и взяты за основу следующие виды угроз и критические активы приведенные в таблице 1 и таблице 2 [2].

Таблица 1.Критерии угроз

№	Угроза
	Утечка доступа другим лицам
	Модифицировано, чтобы его нельзя было использовать
	Возникшие проблемы из-за третьего лица
	Стихийные бедствия
	Безвозвратно уничтожены или временно утеряны

Таблица 2 Критические активы

	Категории	Актив
	Аппаратное обеспечение	Брандмауэр

		Маршрутизатор Коммутатор Хост машина Хранилище данных
	Программное обеспечение	Антивирус
	Система	Система электронной почты Система базы данных
	Информация	Сервер доступа к информации База данных доступа к информации Аккаунт электронной почты для доступа к информации

В большинстве моделей безопасности используются разные термины для описания обеспечения безопасностью критически важных характеристик, например цели безопасности, аспектов безопасности, служб безопасности и т.п.

2. **Критерии измерения воздействия рисков.** На данном этапе определяются воздействия на активы информационных технологий и выполняются сопоставление с уровнем воздействия угроз. Оценка рисков определяется на основе вероятности угроз в следующем виде [2]:

$$X = X_{\text{угроза}} * X_n * C * \frac{K_0 + K_t}{2} * 100\% \quad (1)$$

где X – количественное значение вероятности угроз, X_n - вероятность невыполнения всех предписаний, C – стоимость ресурса, K_0 - возможность применения правовых уязвимостей, K_t - возможность применения инженерно-технических уязвимостей.

3. **Определение проблемной области**. На этом этапе разрабатываются компонены, которые помогают обнаруживать угрозы, угрожающие утечкой информации в организациях. Сценарии угроз формируются из нежелательных участников, инструментов, мотивов и результатов. *Л*юбая проблемная область порождают последствия, которые соответственно будут оцениваться. Внизу будут приведены примеры проблемных областей [3]:

1. ***Аппаратное обеспечение***. Возникновение повреждения компонентов устройств. Ошибка установки программы из-за несовместимости компонентов или пользовательских устройств.

2. ***Программное обеспечение.*** Отсутствие контроля за использование той или иной программы.

3. ***Система***. Сбой системы по различным причинам, например из-за обновления системы. Также нарушение работоспособности системы по причине не правильных манипуляций пользователя при использовании системы.

4. ***Информация***. Использование пользователем общеизвестных или утекших паролей.

4. **Относительная оценка угрозы**. Чем выше относительная оценка угрозы, тем выше уровень возникновения угроз и влияния их на активы организации.

5**. Осуществляется оценивание**, в котором определяются выполнение требований в рамках кибербезопасности и применяется методы тестирования для определения защищенности информации. Методы тестирования: Brute force; Фишинг по электронной почте со ссылкой перехода; Фишинг по электронной почте посредством вредоносных программ; Конфигурацие файла; Резервирование; Поиск уязвимостей; Поиск пропущенной конфигурации.

При исследовании методов и моделей оценки защищенности информации были отмечены вышеуказанные этапы исследования и были рассмотрены алгоритмы, показатели и критерии эффективного функционирования систем управления информационной безопасности.

Модели системы безопасности включает в себя область угроз, систему защиты, набор барьеров, множество уязвимостей и защищаемую область, а соответственно уязвимость представляет собой возможную реализацию угрозы в отношении защищаемых объектов [2]. Соответственно в барьерах нейтрализируются уязвимости. Таким образом, вычисление и определение данных показателей помогает оценить защищенность системы и информации в целом.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

В процессе изучения данного вопроса были рассмотрены предыдущие работы, выполнены вышеописанные шаги, применены инструменты для анализа защищенности и работоспособности системы и произведены различные виды тестирования на возможность проникновения или получения удаленного доступа. Результаты исследования позволяют предположить, что обеспечение защиты информации и информационной безопасности требуют системного подхода, так как необходимо постоянно совершенствовать модули систем для полноценного функционирования систем защиты. В настоящее время организации покупают готовые программные решения в области информационной безопасности и внедряют системы управления информационной безопасности, но и действия сотрудников имеет прямое влияние на защищенность информации.

ВЫВОДЫ

По анализу защищенности информации можно утверждать, что самыми главными аспектами считаются угрозы и атаки на системы компании. Соответственно у организациях возрастает необходимость проводить оценки

систем безопасности и их соответствие требованиям, минимизировать уровень риска и обеспечить непрерывность производства. В данной работе были рассмотрены вопросы обеспечения защищенности данных, средства контроля защиты информации и возможности оценки рисков, также определены и выполнены анализ уязвимостей с применением инструментов тестирования.

СПИСОК ЛИТЕРАТУРЫ

1. Dhillon G. Information Security - Text & Cases. Burlington, USA: Prospect Press; 2017.
2. Миков Д.А., Булдакова Т.И., Сюзев В.В., Смирнова Е.В., Бауман Ю.И. Модели оценки защищённости данных в информационно-управляющих системах реального времени // Проблемы современной науки и образования. – 2019.
3. Khairur Razikin, Benfano Soewito Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework // Egyptian Informatics Journal. – 2022. – p. 383–404.

АҚПАРАТТЫҢ ҚАУІПСІЗДІГІН БАҒАЛАУДЫҢ МОДЕЛЬДЕРІ МЕН ӘДІСТЕРІ

Аннотация. Ақпараттық қауіпсіздік және ақпараттың қорғалуы жан-жақты пәнаралық байланысы бар өзекті сала болып табылады. Бұл мақалада ақпараттың қауіпсіздігін бағалаудың модельдері мен әдістері қарастырылды, сонымен қатар қауіпсіздік мәселелері және қауіпсіздікті бақылау құралдары сипатталды, мәліметтерді жинау, тәуекелдердің әсерін өлшеу критерийлері, проблемалық аймақты анықтау, қауіптің салыстырмалы бағасы және киберқауіпсіздік шеңберінде талаптардың орындалуын анықтайтын бағалау қарастырылды. Барлық ұйымдар көптеген деректерді сақтайды, онда өндірілген өнімдер, бизнес-процестер және тұтынушылар туралы ақпаратқа ие, тиісінше, деректерді қорғау және қауіпсіздікті қамтамасыз ету қажеттілігі туындайды. Бұл зерттеудің мақсаты-ақпараттың қауіпсіздігін бағалау және ақпараттық қауіпсіздікті басқару тәсілдерін зерттеу. Ақпараттың қауіпсіздігін талдай отырып, ең маңызды аспектілер компания жүйелеріне қауіп-қатер мен шабуылдарды анықтау болып саналады. Тиісінше, ұйымдарда қауіпсіздік жүйелерін бағалау және олардың талаптарға сәйкестігі, тәуекел деңгейін азайту, осылайша өндірістің үздіксіздігін қамтамасыз ету қажеттілігі артады.

Түйінді сөздер: ақпараттық қауіпсіздік, ақпараттың қорғалуы, қауіп, осалдық.

MODELS AND METHODS OF INFORMATION SECURITY ASSESSMENT

Annotation. Information security and information security is an urgent area with a comprehensive interdisciplinary connection. This article discusses models and methods for assessing information security, highlights security issues and describes security controls, discusses steps that include data collection, risk impact measurement criteria, identification of a problem area, relative threat assessment and assessment that determines compliance with cybersecurity requirements, since all organizations store a lot of data that they contain information about manufactured products, business processes and customers, accordingly, there is a need to protect and ensure data security. The purpose of this study is to study approaches for assessing information security and information security management. Analyzing the security of information, the most important aspects are the identification of threats and attacks on the company's systems. Accordingly, organizations have an increasing need to assess security systems and their compliance with requirements, minimize the level of risk, thereby ensuring the continuity of production.

Keywords: information security, information security, threat, vulnerability.