**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

**«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ**

**Студенттер мен жас ғалымдардың**
# «ǴYLYM JÁNE BILIM - 2023»
**XVIII Халықаралық ғылыми конференциясының**
**БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ**
**XVIII Международной научной конференции**
**студентов и молодых ученых**
# «ǴYLYM JÁNE BILIM - 2023»

**PROCEEDINGS**
**of the XVIII International Scientific Conference**
**for students and young scholars**
# «ǴYLYM JÁNE BILIM - 2023»

**2023**
**Астана**

**УДК 001+37**
**ББК 72+74**
**G99**

**«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.**

**ISBN 978-601-337-871-8**

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

**УДК 001+37**
**ББК 72+74**

**ISBN 978-601-337-871-8**

жүйесінің архитектурасы, оның тиімді қолданыстағы жақтары, негізгі сипаттамалары қарастырылды. Соның негізінде ақпараттық қауіпсіздік оқиғаларын жинау және корреляциялау жүйесі жасалды. SIEM жүйесінің енгізілуінен кейін корпоративтік желінің құрылымдық схемасы қалай бейнеленетіндігі көрсетілді. Ақпараттық қауіпсіздік тәуекелдері есептелініп, олардың міндеті нақты қауіптерді түсіну, тәуекелдерді есептеу, сондай– ақ оларды азайтуға және қорғауға бағытталған шараларды таңдау екендігіне көз жеткізілді. Осылардан шығатын негізге ой – SIEM жүйесі зерттеулердің жаңа бағыттарын айқындайтын өзекті ғылыми міндет болып табылатындығын көрсетеді.

Пайдаланылған әдебиеттер:

1. Канев А.Н. Мониторинг событий и обнаружение инцидентов безопасности с использованием SIEM – систем. Международный студенческий научный вестник. – 2015. – № 3;
2. Дмитрий Хамакев «SIEM: ответы на часто задаваемые вопросы», https://habrahabr.ru/post/172389/
3. Максим Гарусев. «Системы корреляции событий: революция или эволюция?», http://www.setevoi.ru/cgi– bin/text.pl/magazines/2003/7/30
4. Артем Медведев «самый безопасный SOC», http://www.jetinfo.ru/stati/samyj– bezopasnyj– soc

УДК 004.056.53

## ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Булкаиров Т.Т[1]., Оспанова С.Т[2]
[1]Л.Н.Гумилев атындағы Еуразия ұлттық университеті, «Радиотехника, электроника және телекоммуникациялар» кафедрасының магистранты, Астана, Қазақстан
[2]Л.Н.Гумилев атындағы Еуразия ұлттық университеті, «Радиотехника, электроника және телекоммуникациялар» кафедрасының лаборанты, Астана, Қазақстан
Научный руководитель – Казиева Н.М.
bulkairov.t@mail.ru

Аннотация: В статье рассматриваются методы защиты информации в телекоммуникационной сети. Проанализированы методы информационной безопасности которые используются для защиты информации в сети. Рассмотрены характеристики методов защиты информации.

Сегодня, когда телекоммуникационная сеть используются для приема и передачи электронной информации. Применение информационных технологий для приема и передачи электронной информации является фактором развития экономики и улучшения функционирование общественных и государственных учреждений, которые необходимо защитить от новых информационных угроз. В целом одним из основных направлений информационной безопасности является прогнозирование, обнаружение и оценка информационных угроз. Также надо отметить то, что применение больших данных привнесло больше науки, удобства и практичности в труде и жизнь людей. Популярность больших данных также делает телекоммуникационные сети объектами для серьезных угроз безопасности. Открытость самой сети позволяет любому пользователю войти в сеть, чтобы просматривать и запрашивать информацию, которая создает большую угрозу информационной безопасности сети. В связи с вышеизложенным существует необходимость более детально рассмотреть методы защиты информации в телекоммуникационной сети. В рамках статьи был произведен обзор статье по этому направлению.

В статье [1] представлен способ изменения разрешенного маршрута потоков данных и реализован дополнительный анализ потоков несанкционированного доступа путем контроля параметров (адреса и порты) узлов, а также введение дополнительных узлов анализа позволяет обеспечить повышение защищенности ITCS и объектов критического важных для инфраструктуры. Авторы статьи представляют способ с помощью, которого можно защитить сеть предприятия от атак со стороны компьютерного интеллекта.

В следующей статье [2] приведены инструкции для настройки сетевых интерфейсов приема и передачи файлов, сбор телеметрической информации и отправка служебных сообщений. Механизмы защиты для протоколов динамической маршрутизации, которые можно условно отнести к протоколам управления, которые влияют на таблицу коммутации, имеют практическое значение. Защита на этом уровне позволяет обеспечить целостность данных пути передачи. Авторы статьи разработали механизмы для безопасной передачи мультимедийных данных, телеметрической информации и отправки служебных сообщений.

В статье [3] исследовались методы о том что с широким применением компьютерных сетей, сетевая безопасность также находится под серьезной угрозой, и информация часто крадется. Поэтому обеспечение информационной безопасности компьютерной сети имеет большое практическое значение. Представлен метод управления безопасностью полетов. Этот метод управления реализуется путем выявления и предотвращения аномальных атак. Наконец, имитационный эксперимент доказывает эффективность метода управления безопасностью, который позволяет точно обнаруживать аномальные атаки и обеспечивать информационную безопасность сети.

В статье [4] рассматривались существенные угрозы, исходящие из интернета, создать эффективно работающую систему безопасности. Первое, что нужно сделать, это провести IT– аудит безопасности данных, подключить программы на ПК, позволяющие сохранить конфиденциальную и любую другую важную для бизнеса или частной жизни информацию. Технических средств и методик более чем достаточно, также можно обеспечить своей компании мониторинг IT– инфраструктуры. Как предлагают авторы только комплексное применение существующих средств и методик защиты может повысить степень безопасности сети предприятия.

Заключение: В телекоммуникационных сетях наиболее надежными считаются криптографические методы защиты информации, так как даже в случае перехвата информации по каналам связи, она будет зашифрована. Этот метод позволяет решить сразу две проблемы защиты данных: проблему конфиденциальность и целостности. Также необходимо разработать механизмы защиты для предприятий индивидуально в зависимости от его деятельности. Однако стоит помнить о том, что возможно обеспечить полную защиту информации в телекоммуникационных сетях только с комплексным применением всех описанных методов. Еще одним из методов защиты являются биометрические, которые сегодня все чаще используются для идентификации и аутентификации.

**Список использованных источников**

1. A.I.Klimenko, U.I.Starodubeev, E.G.Balenko The Protection Method for Telecommunication Networks from the Computer Intelligence // International Science and Technology Conference "EastConf". 2019 P. 3

2. S.Lebedev, A.Kollerov, A.Fartushnyi The Security Profiles` Formation Peculiarities of Telecommunication Equipment at Objects of Critical Information Infrastructure // Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 2021 P. 4

3. L.Zhaoyu, Research on computer network information security management and protection strategy // International Conference on Computers, Information Processing and Advanced Education (CIPAE). 2022 P. 4

4. L.T. Mavlyanova Protection of information on the internet // Scientific Journal Impact Factor. VOLUME 2 | ISSUE 1. 2021 P.