БЕЗПЕКА ІНФОРМАЦІЇ
2021, vol. 27, issue 1

http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

Alternative serial title: ***Ukrainian Scientific Journal of Information Security***

ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
Key title: ***Bezpeka ìnformacìì***
Abbreviated key title: ***Bezpeka ìnf.***

Науковий журнал «Безпека інформації» засновано у 1995 році. Засновником та видавцем є Національний авіаційний університет (м. Київ, Україна). Основною метою журналу є висвітлення результатів наукових досліджень та поширення інформації з усіх аспектів інформаційної безпеки. Журнал виходить три рази на рік українською, англійською та російською (змішаними) мовами. Категорії читачів: студенти, аспіранти, докторанти, викладачі, науковці та фахівці у галузі інформаційної безпеки. У журналі можуть публікуватися виключно оригінальні, раніше не опубліковані статті у галузі інформаційної безпеки. Усі статті, опубліковані у журналі, рецензуються членами редакційної колегії або уповноваженими експертами. Редакція може не поділяти думок авторів. Відповідальність за науковий зміст поданих матеріалів несуть виключно автори.

Ukrainian Scientific Journal of Information Security was established in 1995. National Aviation University (Kyiv, Ukraine) is the founder and publisher of the journal. The main aim of the journal is to highlight the results of scientific researches and the dissemination of information on all information security aspects. Journal is published three times (issues) a year in Ukrainian, English & Russian (mixed languages). Categories of readers: students, postgraduate students, doctoral candidates, researchers & experts in information security. Journal publishes only original unpublished articles in information security. All papers published in journal are reviewed by members of Editorial Board or by appointed experts. Editorial Board may disagree with the authors. Authors are responsible for the scientific content of submitted materials.

Научный журнал «Безопасность информации» основан в 1995 году. Учредителем и издателем является Национальный авиационный университет (г. Киев, Украина). Основной целью журнала является освещение результатов научных исследований и распространение информации по всем аспектам информационной безопасности. Журнал выходит три раза в год на украинском, английском и русском (смешанных) языках. Категории читателей: студенты, аспиранты, докторанты, преподаватели, ученые и специалисты в области информационной безопасности. В журнале могут публиковаться исключительно оригинальные, ранее не опубликованные статьи в области информационной безопасности. Все статьи, опубликованные в журнале, рецензируются членами редакционной коллегии или уполномоченными экспертами. Редакция может не разделять мнений авторов. Ответственность за научное содержание представленных материалов несут исключительно авторы.

Зареєстровано Державною реєстраційною службою України (Свідоцтво КВ № 18940-7730 ПР від 25 травня 2012 р.)

Рекомендовано до друку Вченою радою Національного авіаційного університету (протокол № 4 від 21 квітня 2021 р.)

Включено до **категорії «Б»** переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора (кандидата) технічних наук (Наказ МОН України № 975 від 11.07.2019).

ABSTRACTED / INDEXED IN: EBSCO*host*, INDEX COPERNICUS, CrossRef, Google Scholar, Ukrainian Journal of Abstracts «Dzherelo», Simple Search Metadata (SSM), Bielefeld Academic Search Engine (BASE), WorldCat (OAIster), ISSN & Ulrich's Periodicals Directory.

Редакційна колегія

Адреса редакційної колегії

03680, УКРАЇНА, м. Київ
проспект Любомира Гузара, 1
Національний авіаційний університет
Кафедра безпеки інформаційних технологій
корпус 11, кімната 424, телефон: +38 (044) 406-76-42
корпус 11, кімната 102, телефон: +38 (044) 406-70-02
Головний редактор проф. Корченко Олександр Григорович
Ел. пошта: ***infosecurity@nau.edu.ua***

Editorial board

Editorial Address

03680, Kyiv, UKRAINE
Liubomyra Huzara ave. 1
National Aviation University
Academic Department of IT-Security
Building 11, Room 424, Phone: +38 (044) 406-76-42
Building 11, Room 102, Phone: +38 (044) 406-70-02
Editor-in-Chief Prof. Oleksandr G. Korchenko
E-mail: ***infosecurity@nau.edu.ua***

Зміст

Contents

Cybersecurity & critical information infrastructure protection

Privacy&protection from identity theft

E-governance security

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.26.15569

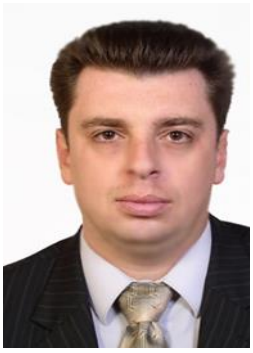
МЕТОДЫ РАСПОЗНАВАНИЯ КИБЕРАТАК С УЧЕТОМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ СРЕДЫ

Хорошко В.А.[1], Браиловский Н.Н.[2]

[1]Национальный авиационный университет
[2]Киевский национальный университет имени Тараса Шевченка

ХОРОШКО Володимир Олексійович, д.т.н., професор.

Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функціонування складних систем.
Публікації: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.



БРАІЛОВСЬКИЙ Микола Миколайович, к.т.н., доцент

Рік народження: 1972, м. Київ, Україна.
Освіта: Українська державна академія зв'язку ім. О.С. Попова, 1994 рік.
Посада: доцент кафедри кібербезпеки та захисту інформації.
Наукові інтереси: національна безпека, методи та засоби технічного захисту інформації, захист кіберпростору, соціальна інженерія.
Публікації: понад 130 наукових публікацій, серед яких наукові статті, колективні монографії, тези та матеріали доповідей на конференціях, підручники та науково-методичні посібники.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.

Аннотация. *На сегодняшний день выявление кибератак является весьма актуальной задачей. Для этой цели используется мониторинг сетей. Причем, при этом возникает необходимость оперативной аналитической обработки информации, требующая применения методов интеллектуального анализа данных. Интеллектуальный анализ данных помогает извлечению знаний из полученных данных. Цель применения интеллектуального анализа данных к решению задач мониторинга кибератак – получение ранее не известных, нетривиальных, доступных для интерпретации процессов знаний, закономерностей в мониторинге, то есть – данных, полезных для поддержания принятия решений. Неотъемлемой частью распознающей системы является обучение, имеющее конечной целью формирование эталонных описаний классов, форма которых определяется способом их использования в решающих правилах, а также выбор информационных признаков для распознавания этих эталонных классов. При написании данной работы сделана попытка изложить в определенной логической последовательности основные аналитические методы распознавания кибератак в современных условиях кибервойны с учетом мониторинга информационной среды. Приведён перечень факторов, подтверждающих целесообразность применения методов распознавания образов для анализа данных мониторинга атак. Кроме того, рассмотрены меры сходства, которые используются в алгоритмах ранжирования и кластеризации кибератак. Показано, что целесообразность их применения зависит от конкретных задач.*

Ключевые слова: *кибератака, мониторинг сетей, методы интеллектуального анализа, методы распознавания образов, системы киберзащиты.*

Вступление

Постоянное возрастание роли информационной сферы на современном этапе характеризует развитие общества. По структуре оно представляет собой совокупность информации, информационных систем и информационных связей объектов, которые производят подготовку информации, ее хранение, распространение и использование, а также процессов регулирования возникающих конфликтов в этих общественных отношениях.

Информационная сфера стала сегодня базой для развития всех других сфер в жизни человека, общества и государства.

В информационной сфере происходят различные события и явления, анализ которых становится жизненно необходимым для любого объекта.

В современных условиях все больше распространяется аксиома, что киберзащита информационных технологий должна по своим характеристикам соответствовать масштабам угроз и рисков. Отклонение от этого правила приведет к дополнительным убыткам. Для каждой информационной системы должен существовать оптимальный уровень киберзащищенности, который необходимо постоянно поддерживать.

Нет сомнений, киберзащита очень важна для информационных систем. Однако нет ответа на очень важный вопрос – насколько решения, которые предлагаются и/или реализуются, действительно соответствуют требованиям киберзащиты.

Всем специалистам в области киберзащиты известны основные постулаты, которые весьма актуальны и на сегодняшний день [1]:

– абсолютной киберзащиты информации создать невозможно;

– система киберзащиты информации должна быть комплексной;

– система киберзащиты информации должна быть адекватной к изменениям обстановки;

– система киберзащиты информации должна быть системою, а не просто набором хаотичных средств;

– системный подход к киберзащите информации должен применяться, начиная с этапа подготовки технического задания и заканчиваться оценкой эффективности и качества системы в процессе ее эксплуатации.

Следует учитывать, что система киберзащиты информации должна иметь целевое назначение. Причем, чем более конкретно сформулирована цель киберзащиты информации, детально выяснены ресурсы, которые имеются и определен комплекс ограничений, тем в большей степени возможно получить позитивный результат.

Однако следует отметить, что основным элементом внешнего воздействия на информационную систему является кибератака.

В последние годы кибератаки (КА) стали широко применяться не только отдельными хакерами или объединенными их в группы, но и государствами структурами некоторых стран.

Так, например, в 2008 году были осуществлены кибератаки Российской федерацией на банковскую систему Эстонии и государственные сайты Грузии, а с 2013 года осуществляются постоянные кибератаки на украинские сайты [2]. В настоящее время одним из самых сложных и полнофункциональных средств проведения атак на информационные системы являются кибератаки, которым присущи следующие функции [2]:

– распространение в сетях;

– перехват сетевых пакетов;

– обнаружение сетевых ресурсов и сбор перечня уязвимых паролей;

– передача информации на серверы злоумышленников;

– сканирование диска информационной системы на наличии определенных расписаний и контента;

– использование большого количества домен для приема команд с серверов управления.

Как сообщает газета The Financial Times, специалисты Центра правительственной связи (GCHQ) разведслужбы, отвечающие за безопасность британских властей, пришли к выводу, что ФСБ России используют программное обеспечение «Лаборатория Касперского» для скрытого наблюдения за сотрудниками правительства и военными Великобритании [1,2].

Кроме того, глава британского Национального центра безопасности (NCSC) заявил, что в 2016 году российские хакеры осуществили кибератаки на СМИ, систему телекоммуникаций и энергетический сектор Великобритании.

И, как сообщает английская газета The Daily Telegraph, глава NCSC отметил, что его ведомство взаимодействует с международными партнерами, представителями индустрии и общественными организациями для решения этой проблемы [1,2].

По данным NCSC с 2016 года его специалистам удалось предотвратить десятки миллионов кибератак. Они также приняли контрмеры в ответ на 590 хакерских атак, в том числе на масштабную кибератаку, происшедшую в мае 2017 года посредством вируса-вымогателя WannaCry, целью которого стала национальная система здравоохранения Великобритании. В этом нападении раньше подозревали хакеров, связанных с КНДР, однако, как пишет издание, имела место угроза, исходящая именно со стороны России [2].

Поэтому, **выявление кибератак является весьма актуальной задачей.** Для этой цели используется мониторинг. Причем, при этом возникает необходимость оперативной аналитической обработки информации, которая требует применения методов интеллектуального анализа данных.

В настоящее время ввод и хранение больших массивов данных мониторинга не представляют актуальных проблем.

На первое место выдвигаются ряд других вопросов: «Поможет ли эта информация выявлению кибератак? Как использовать «историю» мониторинговых данных, чтобы выявить кибератаки? Можно ли предсказать поведение таких процессов? и т.д.».

Эти вопросы становятся особенно важными при наличии больших массивов разнородных данных, какими являются данные мониторинга КА. По этой причине, интеллектуальный анализ данных помогает извлечению знаний из полученных данных. Цель применения интеллектуального анализа данных к решению

задач мониторинга КА – получение ранее не известных, нетривиальных, доступных для интерпретации процессов знаний, закономерностей в мониторинге, то есть – данных, полезных для поддержания принятия решений.

В литературе приводится классификация задач интеллектуального анализа данных по типам производимой информации [3,4] выделяя при этом пять основных видов задач.

1.Классификация (распознавание с «учителем») – наиболее распространённая задача интеллектуального анализа данных. Она позволяет выявить признаки, характеризующие однотипные группы КА – классы, для того, чтобы по известным значениям их характеристик можно было отнести к тому или иному классу. Ключевым моментом выполнения этой задачи является анализ множества классифицированных атак. В качестве методов решения задачи классификации могут использоваться различные алгоритмы [5,6], байсовские сети [7,8], индукция деревьев решений, индукция символьных правил [9,10], нейронные сети [11], параметрические алгоритмы распознавания [12] и другие.

2.Кластеризация. Результатом кластеризации является определение присущего исследуемым данным разбиения на кластеры. В большинстве случаев кластеризация субъективна, т.к. любой вариант разбиения на кластеры напрямую зависит от выбранной меры расстояния между кластеризуемыми атаками [3,13,14].

3.Выявление ассоциаций. Ассоциация определяется на основе свойств двух или нескольких одновременно наступающих событий. При этом производные правила указывают на то, что при наступлении одного события с той или иной степенью вероятности наступит и другое. Количественно сила ассоциации определяется несколькими величинами: предсказуемость, распространяемость и ожидаемая предсказуемость [15].

4.Выявление последовательностей. Подобно ассоциациям, последовательность имеет место между событиями, но наступающими не одновременно, а с некоторым определенным интервалом во времени. Таким образом, ассоциация является частным случаем последовательности с нулевым временным шагом [15,16].

5.Прогнозирование – на основе особенностей поведения текущих и предыдущих данных оцениваются будущие значения определенных числовых показателей. В задачах подобного типа наиболее часто используются традиционные методы математической аналитики, а также нейронные сети [17-21].

Целью данной работы является анализ и изложение в определенной логической последовательности основных аналитических методов распознавания кибератак в современных условиях кибервойны с учетом мониторинга информационной среды.

Основная часть

Пусть $X = \{x_1, x_2, \dots, x_n\}$ – начальное множество КА. Каждая атака, которая может быть осуществлена на информационную систему, описывается набором характеристик свойств-признаков $X' = (x_{i1}, x_{i2}, \dots, x_{im})$, i= *1,2,…,n*. Геометрически атаку удобно интерпретировать точкой или вектором в соответствующем m-мерном пространстве (информационной сфере). Строго говоря, такое описание атаки представляет собой ее образ.

Распознаванию подлежат не собственно атаки, а образы – формализованные понятия, с которыми ассоциируется КА. В дальнейшем для краткости изложения под термином «кибератака» будем понимать образ атаки.

Наличие определенной общности свойств у разных типов атак позволяет группировать атаки в некоторые подмножества $K_1, K_2, \dots, K_k$ множества X-классы.

Распознаваемые образы можно определить как отношения исходных атак $\{x_1, x_2, \dots, x_n\}$ к определенному классу K_j, j=*1,2,…,k*, с помощью выделения существенных признаков или свойств, характеризующих эти атаки. Это означает, что нужно построить однозначное отображение множества X на множестве классов $K = \{K_1, K_2, \dots, K_k\}; X \to K$.

Все k исследуемых классов представлены непересекающимися множествами своих «представителей»:

$$\{X_1^{(j)}, X_2^{(j)}, \dots, X_{n_k}^{(j)}\} \subset K_j; j = 1,2, \dots, k;\ n_1 + n_2 + \dots + n_k = n_0,$$

так называемыми обучающими выборками. Насколько хорошо атаки обучающих выборок отражают постоянную структуру классов, дает понятие представительности выборки.

Формально представительность обычно оценивается отношением n_j/m, где n_j – число атак в выборке, а m – размерность признакового пространства.

Используя информацию, содержащуюся в обучающейся выборке и, может быть, некоторые априорные данные о решаемой задаче, требуется построить решающее правило, наилучшим образом классифицирующее атаки распознавания.

Обычно решающее правило определяется разделяющей функцией R(x), которая в случае безошибочного разделения двух классов ведет себя следующим образом:

R(x)>0 для x ⊂ K_1,

R(x)<0 для x ⊂ K_2.

К априорным данным о решаемой задаче относятся:

- желаемая размерность;
- вероятностная ситуация;
- детерминированная ситуация;
- контрольная выборка.

Желаемая размерность. Под этим понятием подразумевается, что известно число признаков, необходимое для решения задачи. Во многих методах число признаков не задается, а определяется в процессе выбора пути оптимизации какого-либо критерия.

Вероятностная ситуация (задан вид распределения). Считается, что атака относится к данному классу с некоторой вероятностью. Такая ситуация порождает статистические методы.

Детерминированная ситуация (вид и параметры распределения не известны). Считается, что классы не пересекаются, т.е., КА различных классов изолированы друг от друга. Такая ситуация порождает непараметрические методы.

Контрольная выборка. Состоит из атак заданных классов:

$$\{X_1^{(j)}, X_2^{(j)}, \dots, X_{n_e}^{(j)}\} \subset K_j; j = 1,2, \dots, k;\ n_1 + n_2 + \dots + n_e = n_q.$$

Контрольные атаки не учитывают в процессе обучения, а используют для оценки качества распознавания. Объекты обучающей и контрольной выробок называют эталонными.

Если затраты, связанные с потерями от неправильного распознавания и с реализацией некоторого решающего правила обозначить С, то четверка множеств {X,K,R,C} будет характеризовать задачу распознавания. Можно выделить три типа задач:

1) задано множество классов K (обычно задается обучающая выборка), пространство признаков X, требуется найти решающее правило R, минимизирующее затраты С. Это задача распознавания при наличии обучения. Простым случаем этой задачи является ранжирование (случай k=1) – упорядочение видов атак по некоторой мере сходства относительно заданного класса;

2) задано множество классов K, решающие правило R, требуется найти систему признаков X, минимизирующих затраты С. Это задача минимизации пространства признаков;

3) задано пространство признаков X, требуется найти множество классов K и решающее правило R. Это задача кластеризации – разбиение атаки на некоторые, в общем случае не заданное, число классов в соответствии со свойствами самих атак.

Однако четверка множеств {X,K,R,C} характеризует тип задачи распознавания формально, так как не учитывает связи между входящими в нее величинами. Поэтому практически все методы распознавания основаны на определенных предположениях. Наиболее распространенными являются следующие [22]:

- о независимости выбора КА;
- о компактности классов;
- о существовании функции признаков каждого класса;
- о линейной разделимости классов;
- о нормальной распределенных матриц классов;
- о независимости признаков.

Использование гипотез такого рода предопределяет выбор алгоритма и качество решения задачи распознавания.

Важным понятием является отказ от распознавания. В сомнительных случаях (атака расположена слишком близко к разделяющей функции) или при нарушении гипотезы компактности (атака расположена далеко от средних значений классов) классификация не производится.

Используя отказ, можно повышать качество распознавания, хотя число правильных решений и уменьшается.

Понятие меры сходства позволяет оценить степень сходства между элементами распознающей системы, т.е. между атаками, классами атак, классом и отдельной КА.

В зависимости от решаемой задачи используется определенная мера сходства.

Неотъемлемой частью распознающей системы является обучение, имеющее конечной целью формирование эталонных описаний классов, форма которых определяется способом их использования в решающих правилах, а также выбор информационных признаков для распознавания этих эталонных классов.

Теперь рассмотрим типы исходных данных мониторинга.

Обозначим через X_i - КА, а через V_j - признаки (свойства, атрибуты) атак $V_j = X_i = (x_1, x_2, \dots, x_n)$ Можно выделить 4 типа исходных данных:

1. Таблица типа «атаки-признаки» (см. рис. 1) - для *n* атак заданы значения *m* признаков в фиксированный момент времени *t*.

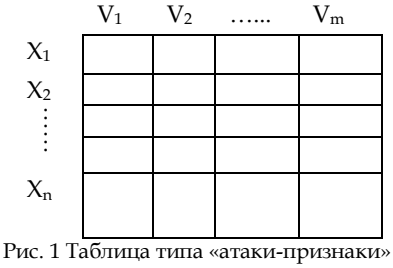


Рис. 1 Таблица типа «атаки-признаки»

2. Таблица значений одного признака (см. рис.2), измеренного в разные моменты времени $t_1, t_2, \dots, t_k$ для *n* атак.

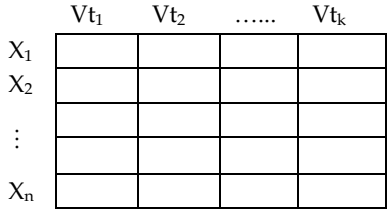


Рис. 2 Таблица значений одного признака

3. Таблица значений признаков одной атаки (см. рис. 3), измеренных в разные моменты времени $t_1, t_2, \dots, t_q$.

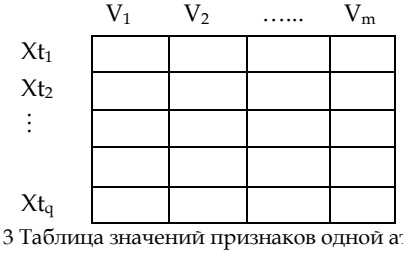


Рис. 3 Таблица значений признаков одной атаки

4. «Куб данных» - значения признаков (см. рис.4), измеренных в разные моменты времени $t_1, t_2, \dots, t_q$ для *n* атак.

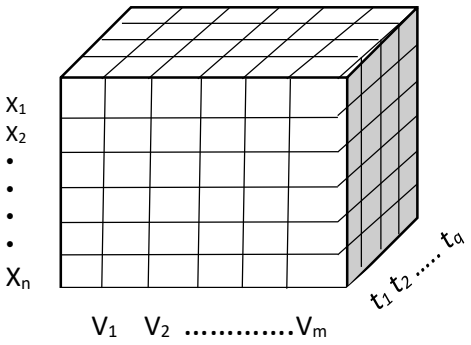


Рис. 4 «Куб данных»

Данные мониторинга характеризуются тем, что могут быть количественными и качественными, иметь разные размерности, пропущенные значения и погрешности измерения, носить сезонный характер, временной характер и т.п. Кроме того, часто переменные имеют разный диапазон измерений, так как измерены они разными методами или просто из-за того, что характеризуют разные свойства КА.

Непосредственное использование переменных в анализе может привести к тому, что классификацию будут определять те из них, которые имеют наибольший разброс значений. Поэтому применяются следующие виды стандартизации [12]:

1) «Z-шкалы». Из значений переменных вычитают их среднее, и эти значения делятся на стандартное отклонение:

$$x_{ij}^* = \frac{x_{ij}-\overline{x_j}}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_{ij}-\overline{x_j})^2}},\ i=1,2,\ldots,n;\ j=1,2,\ldots,m.$$

2) «Разброс от 0 до 1». Линейным преобразованием переменных добиваются разброса значений от 0 до 1:

$$x_{ij}^* = \frac{x_{ij}-\min\limits_i x_{ij}}{\max\limits_i x_{ij}-\min\limits_i x_{ij}}.$$

3) «Максимум-1». Значения переменных делятся на их максимум:

$$x_{ij}^* = \frac{x_{ij}}{\max\limits_i x_{ij}}.$$

4) «Средние-1»: Значения переменных делятся на их среднее:

$$x_{ij}^* = \frac{x_{ij}}{\overline{x_{ij}}}.$$

5) «Стандартное отклонение – 1». Значение переменных делится на стандартное отклонение:

$$x_{ij}^* = \frac{x_{ij}}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_{ij}-\overline{x_j})^2}}.$$

6) «Разброс от -1 до 1». Линейным преобразованием переменных добиваются разброса значений от -1 до 1:

$$x_{ij}^* = \frac{2x_{ij}-\min\limits_i x_{ij}-\max\limits_i x_{ij}}{\max\limits_i x_{ij}-\min\limits_i x_{ij}}.$$

7) Центрирование и масштабирование на среднее значение:

$$x_{ij}^* = \frac{x_{ij}-\overline{x_j}}{\overline{x_j}}.$$

Теперь рассмотрим меры сходства [23]

Причем, меры сходства двух элементов Z_i и Z_j определяются некоторой функцией $d(Z_i, Z_j)$, обладающей следующими свойствами:

1. Симметрия

$$d(Z_i, Z_j) = d(Z_j, Z_i);$$

2. Максимальное сходство элемента с самим собой

$$d(Z_i, Z_j) = 0, d(Z_i, Z_j) > 0, i \neq j.$$

Мера, удовлетворяющая этим свойствам, называется расстоянием, если выполняется неравенство треугольника

$$d(Z_i, Z_j) < d(Z_i, Z) + d(Z, Z_j).$$

Приведем наиболее распространенные меры сходства [3,12,14,23].

Узловым моментом в кластерном анализе считается выбор меры сходства атак, от которой решающим образом зависит окончательный вариант разбиения атак на группы при заданном алгоритме разбиения.

В каждом конкретной задаче этот выбор производится по-своему, с учетом главных целей исследования. Основные меры сходства между КА:

1) евклидово расстояние

$$d_E(X_i, X_j) = \left[\sum_{i=1}^{m}(x_{i1}-x_{j1})^2\right]^{1/2}; \quad (1)$$

2) взвешенное евклидово расстояние

$$d_B(X_i, X_j) = \left[\sum_{i=1}^{m}\omega_1(x_{i1}-x_{j1})^2\right]^{1/2}, \quad (2)$$

где ω_1 - весовой коэффициент;

3) потенциальная функция

$$d_\Pi(X_i, X_j) = \left[1+\propto d_E^2(X_i, X_j)\right]^{-1};\ \propto > 0 \quad (3)$$

$$\text{или } d'_\Pi(X_i, X_j) = \exp\left[-\propto d_E^2(X_i, X_j)\right] \quad (4)$$

$$\text{или } d''_\Pi(X_i, X_j) = \left|\frac{\sin d_E^2(X_i, X_j)}{\propto d_E^2(X_i, X_j)}\right|; \quad (5)$$

4) угол между векторами X_i и X_j

$$d(X_i, X_j) = arccos\frac{X_i * X_j}{|X_i| * |X_j|}. \quad (6)$$

Теперь рассмотрим меры сходства между классами.

1) Максимальное из исходных расстояний между КА разных классов

$$d_{min}(K_i, K_j) = \min d(X_1, X_m);\ X_1 \in K_i, X_m \in K_j\ . \quad (7)$$

2) Максимальное из исходных расстояний между КА равных классов

$$d_{max}(K_i, K_j) = \max d(X_1, X_m);\ X_1 \in K_i, X_m \in K_j\ . \quad (8)$$

3) Среднее значение парных расстояний между атаками разных классов

$$d_{mean}(K_i, K_j) = \frac{1}{n_i \cdot n_j}\sum_{X_1 \in K_i}\sum_{X_m \in K_j} d(X_1, X_m). \quad (9)$$

4) Расстояние, измеряемое по «центрам тяжести» классов

$$d_c(K_i, K_j) = d_E(\mu_i, \mu_j), \quad (10)$$

где $\mu_1 = \frac{1}{n_1}\sum_{X_j \in K_1} X_j$– вектор средних классов K_1.

5) Потенциальная функция

$$d_\Pi(K_i, K_j) = \frac{1}{n_i \cdot n_j}\sum_{X_1 \in K_i}\sum_{X_m \in K_j} d_\Pi(X_1, X_m). \quad (11)$$

6) Обобщенное (по Колмогорову) расстояние

$$d_K(K_i, K_j) = \left[\frac{1}{n_i \cdot n_j}\sum_{X_1 \in K_i}\sum_{X_m \in K_j} d_E^q(X_1, X_m)\right]^{1/q}. \quad (12)$$

Расстояния $d_{min}(K_i, K_j)$, $d_{max}(K_i, K_j)$, $d_{mean}(K_i, K_j)$ являются частными случаями обобщенного расстояния:

при $q \to \infty$ $d_K(K_i, K_j) = d_{max}(K_i, K_j)$,

при $q \to -\infty$ $d_K(K_i, K_j) = d_{min}(K_i, K_j)$,

при $q \to 1$ $d_K(K_i, K_j) = d_{mean}(K_i, K_j)$.

Рассмотрим теперь меры сходства между атаками и классами [23]:

1) Расстояние Махаланобиса

$$d_M(X, K_i) = (X-\mu_i)^T C_i^{-1}(X-\mu_i), \quad (13)$$

где μ_i и Ci – соответственно вектор средних и ковариационная матрица класса K_i;

2) Функция меры близости

$$d_{\text{ФМБ}}(X, K_i) = \left[\prod_{X_j \in K_i} d(X, X_j)\right]^{1/n_i}, \quad (14)$$

$$d_{\text{ФМБ}}(X, K_i) = \frac{1}{n_i}\sum_{X_j = K_i} \ln d(X, X_j),$$

где $d(X, X_j)$ – мера сходства между атаками, например, евклидово расстояние;

3) Потенциальная функция

$$d_\Pi(X, K_j) = \frac{1}{n_i}\sum_{X_j \in K_i} d_\Pi(X, X_j)\ , \quad (15)$$

где $d_\Pi(X_1, X_m)$ –определяется выражением (3);

4) Угловая мера подобия

$$d_{PSI}(X, K_i) = \left[\prod_{X_j \in K_i} sin(X \wedge X_j)\right]^{1/n_i}, \quad (16)$$

где $(X \wedge X_j)$ –угол между векторами X и X_j;

5) Расстояние до «центра тяжести» класса

$$d_c(X, K_i) = d_E(X, \mu_i), \quad (17)$$

где μ_i - вектор средних класса K_i;

6) Проекция на подпространство

$$d_{LS}(X, \pi_i) = \frac{|X_0|}{X}, \quad (18)$$

где $X_0 = \sum_{X_j \in K_i} \alpha_i X_i$ - проекция на гиперплоскость Г, натянутую на I ($I<n_i$) линейно независимых атак класса K_i,

$I<m$, m – размерность пространства,

α_j – коэффициенты, находятся из условия ортогональности (X-X_0, X_j)=0, j=1,2,…,I, $X_j \in K_i$.

Мера различия, соответствующая $d_{LS}(X, K_i)$

$$d_{LS}(X, K_i) = |X - X_0| \Big/ |X| = [|X|^2 + |X_0|^2 - 2(X, X_0)]^{1/2} \Big/ |X|. \quad (19)$$

Выводы

Целесообразность применения методов распознавания образов для анализа данных мониторинга КА обусловлена следующими факторами:

1. Одни и те же методы распознавания образов можно использовать для широкого класса различных по содержанию задач.

2. Класс используемых в анализе данных мониторинга методов распознавания образов обширен. Это методы ранжирования КА (признаков КА), методов распознавания «с учителем», методы кластеризации, методы группового учета аргументов. Каждой группе методов распознавания соответствует определенные задачи мониторинга. Но при этом в каждом конкретном случае применяются методы, учитывающие особенности исходных данных.

3. Применение методов распознавания образов позволяет проводить комплексный анализ разнородных данных, которые получают в процессе мониторинга.

Кроме того, рассмотренные меры сходства используются в алгоритмах ранжирования и кластеризации КА. Целесообразность их применения зависит от конкретной задачи.

В частности, евклидовое расстояние лучше использовать для количественных переменных, расстояние хи-квадрат – для исследования частотных таблиц, а также имеется множество мер для бинарных переменных.

Литература

[1] Грищук Р.В. *Основи кібернетичної безпеки*/ Р.В. Грищук, Ю.Г. Даник – Житомир: ЖНАЕУ, 2016. – 616 с.

[2] Пирцхалава Л.Г. *Информационное противоборство в современных условиях*/ Л.Г. Парцхалава, В.А. Хорошко, Ю.Е. Хохлачева, М.Е. Шелест – К: ЦП «Компринт», 2019- 226 с.

[3] Дюк В. *Data Mining* / В.Дюк, А. Сомойленко – СПб: Питер, 2001 – 368 с.

[4] Fuernkranz J. A *Brief Introduction to Knowledge Discovery in Databases* // OEGAI Journal. - 2005. - № 14(4). – pp. 14-17.

[5] Ту Дж *Принципы распознавания образов*. Изд. 2-е / Дж Ту, Р. Гонсалес – М.: Мир, 2001. – 412 с.

[6] Фукунага К. *Введение в статистическую теорию распознавания образов*. Изд. 3-е допол. / К. Фукунага – М.: Наука, 2005. – 388 с.

[7] Тулупьев А.Л. *Алгебраические байесовские сети. Логико-вероятностный подход к моделированию баз знаний с неопределенностью* / А.Л. Тулупьев – СПб.: СПИИРАН, 2000. – 292 с.

[8] Friedman N., Geiger D., Goldszmidt M., etc. *Bayesian Network Classifiers*//Machine Learning.-2007.-pp. 131-165.

[9] Michalski R. S. *A theory and methodology of inductive learning*//Artificial Intelligence.-1999.-20(2). - pp.111-162.

[10] Quinlan J. R. *Induction of decision trees* // Machine Learning. - 2006. - №1. - pp. 81-106.

[11] Fausett L. V. *Fundamentals of Neural Networks: Architectures, Algorithms, and Applications*. - Englewood Cliffs, New Jersey: Prentice Hall, 1994. - 461 p.

[12] *Классификация многомерных наблюдений Изд. 2-е* / С.А. Айвазян, З.И. Бежаева, О.В. Староверов. - Москва: Статистика, 2001. – 244 с.

[13] Дюран Б., Оделл П. *Кластерный анализ*. Изд. 3-е доп./Б. Дюран, П. Оделл.-М.: Статистика,2007.–128 с.

[14] Жамбю М. *Иерархический кластер-анализ и соответствия*. Изд. 2-е доп. / М. Жамбю — М.: Финансы и статистика, 2002.— 345 с.

[15] *Представление и использование знаний* / Под. Ред. Х. Уэно, М. Исидзука – М.: Мир, 1999. – 220 с.

[16] Muller, J.-A., Lemke, F. *Self-Organizing Data Mining. An Intelligent Approach to Extract Knowledge from Data*. Berlin, Dresden, 1999. – 225 p.

[17] Ивахненко А.Г. *Долгосрочное прогнозирование и управление сложными системами*. – К: Техніка, 1975. – 312 с.

[18] Себер Дж. *Линейный регрессионный анализ*. Изд. 3-е допол. /Дж Себер - М.: Мир, 2005.- 475 с.

[19] Дубровский С.А. *Прикладной многомерный статистический анализ*. Изд. 2-е / С.А. Дубровский – М.: Финансы и статистика, 2002. – 236 с.

[20] Елисеева И. И., Юзбашев М. М. *Общая теория статистики* / Под ред. чл.-корр. РАН И. И. Елисеевой. - М.: Финансы и статистика, 2006. – 368 с.

[21] Кондрашина Е.Ю., Литвинцева Л.В., Поспелов Д.А. *Представление знаний о времении пространстве в интеллектуальных системах* / Под ред. Д.А. Поспелова. - М.: Наука,1999. – 328 с.

[22] Фор А. *Восприятие и распознавание образов*. - М., Машиностроение, 1989. – 302 с.

[23] Раушенбах Г.В. *Меры близости и сходства* // Анализ нечисловой информации в социологических исследованиях. М.: Наука, 1985. – С. 169-203.

УДК 004.681.3

Хорошко В.О., Браіловський М.М. Моніторинг кібератак.
Анотація. *На сьогоднішній день виявлення кібератак є вельми актуальним завданням. Для цієї мети використовується моніторинг мереж. Причому, при цьому виникає необхідність оперативної аналітичної обробки інформації, що вимагає застосування методів інтелектуального аналізу даних. Інтелектуальний аналіз даних допомагає вилучення знань з отриманих даних. Мета притрансформаційних змін інтелектуального аналізу даних до вирішення завдань моніторингу кібернетичних атак - отримання раніше невідомих, нетривіальних, доступних для інтерпретації процесів знань, закономірностей в моніторингу, тобто - даних, корисних для підтримки прийняття рішень. Невід'ємною частиною системи, що розпізнає є навчання, що має кінцевою метою формування еталонних описів класів, форма яких визначається способом їх використання у вирішальних правилах, а також вибір інформаційних ознак для розпізнавання цих еталонних класів. Під час написання даної роботи зроблена спроба викласти в певній логічній послідовності основні аналітичні методи розпізнавання кібернетичних атак в сучасних умовах кібернетичної війни з урахуванням моніторингу інформаційного середовища. Наведено перелік факторів, що підтверджують доцільність застосування методів розпізнавання образів для аналізу даних моніторингу атак. Крім того, розглянуті заходи подібності, які використовуються в алгоритмах ранжирування і кластеризації кібератак. Показано, що доцільність їх застосування залежить від конкретних завдань.*
Ключові слова: *кібератака, моніторинг мереж, методи інтелектуального аналізу, методи розпізнавання образів, системи кіберзахисту.*

Khoroshko V.O., Brailovskyi M.M. Cyber attack monitoring.
Abstract. *To date, the detection of cyberattacks is a very important task. Network monitoring is used for this purpose. Moreover, there is a need for rapid analytical processing of information, which requires the use of methods of data mining. Data mining helps to extract knowledge from acquired data. The purpose of applying data mining to solving problems of monitoring cybernetic attacks is to obtain previously unknown, non-trivial, understandable processes of knowledge, patterns in monitoring, i.e., data useful for supporting decision-making. An integral part of the recognition system is training, which has the ultimate goal of forming reference class descriptions, the form of which is determined by the way they are used in decision rules, as well as the choice of information features for recognizing these reference classes. During the writing of this paper, an attempt was made to set out in a certain logical sequence the main analytical methods for recognizing cyberattacks in modern conditions of cyber warfare, taking into account the monitoring of the information environment. The list of factors confirming expediency of application of methods of recognition of images for the analysis of data of monitoring of attacks is given. In addition, similarity measures used in cyberattack ranking and clustering algorithms are examined. It is shown that the expediency of their application depends on specific tasks.*
Keywords*: cyberattack, network monitoring, methods of intellectual analysis, methods of pattern recognition, cyber defense systems.*

Хорошко Володимир Олексійович, д.т.н., професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Хорошко Владимир Алексеевич, д.т.н., профессор, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Khoroshko Volodymyr, Doctor of Technical Sciences, Professor, Professor of the Department of Information Technology Security of the National Aviation University.

Браіловський Микола Миколайович, к.т.н., доцент, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Браиловский Николай Николаевич, к.т.н., доцент, доцент кафедры кибербезопасности и защиты информации Киевского национального университета имени Тараса Шевченко.
Brailovskyi Mykola, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cyber Security and Information Protection of the Taras Shevchenko National University of Kyiv.

Отримано *22 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*

ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.26.15573

БАЗОВА МНОЖИНА УЗАГАЛЬНЕНИХ КРИТЕРІЇВ ВІДНЕСЕННЯ ОБ'ЄКТІВ ДО КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Юрій Дрейс, Леонід Деркач

Національна академія СБ України, Україна

ДРЕЙС Юрій Олександрович, к.т.н., доцент.

Рік та місце народження: 1984 рік, смт. Червоноармійськ, Житомирська область, Україна.
Освіта: Житомирський військовий інститут радіоелектроніки ім. С.П. Корольова, 2007 рік.
Посада: старший науковий співробітник Національної академії СБ України з 2019 року.
Наукові інтереси: охорона державної таємниці, захист інформації з обмеженим доступом, критична інформаційна інфраструктура, інформаційна та кібербезпека.
Публікації: понад 100 наукових публікацій, серед яких підручник, навчальні посібники, методичні рекомендації, наукові статті та авторські свідоцтва на комп'ютерні програми.
E-mail: academy@ssu.gov.ua.
ORCID: 0000-0003-2699-1597.

ДЕРКАЧ Леонід Васильович

Рік та місце народження: 1939 рік, м. Дніпро, Україна.
Освіта: Дніпровський національний університет імені Олеся Гончара, 1970 рік.
Посада: старший науковий співробітник Національної академії СБ України.
Наукові інтереси: національна та державна безпека.
Публікації: понад 10 наукових публікацій та праць.
E-mail: academy@ssu.gov.ua.
ORCID: 0000-0002-2078-0003.

Анотація. *Відсутність реєстрів об'єктів критичної інфраструктури держави та їх інформаційно-телекомунікаційних систем призводить до невизначеності у кількості необхідних ресурсів для забезпечення їх захисту від можливих кібератак. З огляду на обмеженість таких ресурсів, важливим і актуальним науково-практичним завданням є визначення повноти та меж пріоритетності кіберзахисту зазначених об'єктів. Формування таких реєстрів відбувається за методикою віднесення об'єктів до критичної інфраструктури держави, основаної у т.ч. на відповідних критеріях, які визначатимуть належність певного об'єкту до такого, що є критичним для держави. Проведений аналіз існуючих критеріїв віднесення об'єктів до критичної інфраструктури держави, показує, що в Україні існує низка інших критеріїв (і які слід також враховувати), задіяних у формуванні реєстрів важливих для держави об'єктів, наприклад «Державний реєстр потенційно небезпечних об'єктів». Отже, пропонується сформувати перелік таких узагальнених критеріїв віднесення об'єктів до критичної інфраструктури держави у вигляді базової множини, яка інтегрує десять ознак з можливістю подальшого розширення. Таку множину можна використати для визначення пріоритетності кіберзахисту інформаційно-телекомунікаційних систем (об'єктів критичної інформаційної інфраструктури) об'єктів критичної інфраструктури держави.*

Ключові слова: *об'єкти критичної інфраструктури держави, множина критеріїв критичності, критична інформаційна інфраструктура.*

Вступ

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту, зв'язку, енергозабезпечення, органів державної влади, які забезпечують національну безпеку та оборону, захист від надзвичайних ситуацій (НС). Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для принципово нових, притаманних суспільству з високим рівнем інформатизації.

Існуюче нормативно-правове забезпечення захисту об'єктів критичної інфраструктури (ОКІ) свідчить про наявність низки проблем в енергетичній, інформаційній та інших сферах [1-3], що мають малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість формування переліку інформаційно-телекомунікаційних систем (ІТС) ОКІ тощо. Крім того, на концептуальному та нормативному рівнях не проведено класифікацію ОКІ держави (ОКІД) [4-7], не сформовано перелік їх ІТС як об'єктів критич-

ної інформаційної інфраструктури (ОКІІ), а також відсутні критерії щодо оцінювання негативних наслідків, до яких може призвести кібератака на ІТС ОКІД [8-11].

Актуальність та новизна

Оскільки ресурси, що направлені на забезпечення кібербезпеки є обмеженими (людські, часові, матеріальні тощо), то необхідно встановити пріоритетність (рівень критичності) тих чи інших об'єктів та їх ІТС для забезпечення їх першочергового захисту. Така оцінка приорітетності можлива за рахунок створення множини критеріїв віднесення об'єктів до ОКІД.

Отже, з метою розробки чіткого механізму визначення повноти та меж критичної інформаційної інфраструктури держави суб'єктами забезпечення її кіберзахисту, актуальним є побудова базової множини узагальнених критеріїв віднесення об'єктів до ОКІД.

Аналіз публікацій та досліджень

Відповідно до [12] критерії та порядок віднесення об'єктів до ОКІ, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України (КМУ).

В зазначеному документі також надано і визначення ОКІ та ОКІІ. Так, з урахуванням [13, 26], до ОКІ можуть бути віднесені підприємства, установи, організації незалежно від форми власності, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах, у сферах життєзабезпечення населення, зокрема, у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, охорони здоров'я; є аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду; є об'єктами потенційно небезпечних технологій і виробництв.

Але, як зазначено у [13], віднесення таких об'єктів до ОКІ відбувається за сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму, а саме: «…існування викликів, ризиків і загроз, що можуть виникати щодо ОКІ; уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і опосередкованих); природним ресурсам загальнодержавного значення; обороноздатності; іміджу країни; масштабності негативних наслідків для держави, які: вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів економіки чи призведуть до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаються на діяльності низки інших секторів; тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави; впливу на функціонування суміжних секторів критичної інфраструктури» [13].

Тобто, відповідно до запропонованого у [13] принципу «віднесення таких об'єктів до ОКІ визначається за сукупністю критеріїв», якщо в об'єкті інфраструктури не визначено хоча б одного із вищенаведених критеріїв, то такий об'єкт не може бути віднесений до ОКІ, що є досить дискусійним і суперечливим твердженням, тому й було виключене з кінцевої редакції [14].

Мета роботи

Виходячи з викладеного, *метою роботи* є формування базової множини узагальнених критеріїв віднесення об'єктів до ОКІ для подальшої оцінки пріоритетності їх кіберзахисту.

Основна частина

Провівши аналіз наукових праць і узагальнення діючих нормативно-правових документів [1-26], пропонується *перелік узагальнених критеріїв віднесення об'єктів до ОКІД* за низкою нижченаведених ознак:

1) За сферою діяльності та надання послуг у секторі критичної інфраструктури (табл. 1) [1-3, 8, 9, 12, 13, 15, 26]:

Таблиця 1

Група	*Елемент*	*Умовні позначення*
Підприємства (об'єкти), установи та організації незалежно від форми власності *{ПУО}*	*{*Комунальні, Аварійно-рятувальної служби, Служби екстреної допомоги населенню*}*; *{*У переліку, що мають стратегічне значення для економіки і безпеки держави*}*; {Потенційно небезпечних технологій і виробництв*}*; *{*Включеними до Державного реєстру потенційно небезпечних об'єктів*}*; *{*Підвищеної небезпеки (у т.ч. перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, природному довкіллю)*}*; *{*Об'єктами державної важливості*}*; *{*Під обов'язковою охороною підрозділами ДСО за договорами*}*; *{*Під охороною і обороною в умовах надзвичайних ситуацій і в особливий період*}*; *{*Національною системою конфіденційного зв'язку*}*; *{*Платіжними системи*}*; *{*Системою екстреної допомоги населенню за єдиним номером 112*}*; *{*Нерухомими об'єктами культурної спадщини*}*	*{К, АРС, СЕД}*; *{ПСЗ}*; *{ПНВ}*; *{ОПН}*; *{ПНО}*; *{ОДВ}*; *{ОО}*; *{ООО}*; *{НСКЗ};{ПС}*; *{СЕД}*; *{НОКС}*

Сектор критичної інфраструктури держави *{СКІ}*	*{*Паливно-енергетичний*}*; *{*Інформаційний (інформаційно-комунікаційних технологій, електронних комунікацій*)}*; *{*Систем життєзабезпечення (Централізованого водопостачання, Водовідведення, Постачання електричної енергії і газу, Виробництва продуктів харчування, Сільського господарства*)}*; *{*Харчової промисловості*}*; {Агропромислового комплексу*}*; *{*Охорони здоров'я*}*; {Фінансовий*}*; {Банківський*}*; *{*Транспорту і пошти*}*; {Промисловість (хімічна, металургійна, оборонна, космічна, авіаційна, суднобудівна*)}*; *{*Цивільного захисту населення та територій*}*	*{ПЕ}; {І};* *{СЖ (ЦВ, В, ЕЕГ, ВПХ, СГ)};* *{ХП};{АП};{ОЗ};* *{Ф}; {Б}; {ТП};* *{П (Х,М,О,К,А,С)};* *{ЦЗ}*

2)За критеріями включення до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг (табл. 2) [17].

3) За сукупністю критеріїв, що визначають їх важливість для реалізації життєво важливих функцій та послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення наслідків до відновлення штатного режиму (табл. 3) [2, 13, 18].

Таблиця 2

Група	*Елемент*	*Умовні позначення*
Щодо зберігання {ЗБ}	*{*Наркотичних засобів, Психотропних речовин, Прекурсорів*}*; *{*Історичних та культурних цінностей загальнодержавного значення*}*	*{НЗ, ПР, П};* *{ІКЦ}*
Щодо виробництва та/або зберігання {ВЗ}	*{*Озброєння, Ракет, Боєприпасів, Вибухових речовин, Вогнепальної зброї, Спортивно-мисливської зброї, Спеціальних засобів заряджених речовинами сльозоточивої та дратівної дії, Засобів активної оборони*}*; *{*Запасів пально-мастильних матеріалів, Речового майна, Продовольчого майна*}*	*{О, Р, ВР, ВЗ, СМЗ, СЗ, ЗАО};* *{ПММ, РМ, ПМ}*
Щодо провадження діяльності {ПД}	*{*Водопостачання населених пунктів з резервуарами питної води*}*; {Захоронення радіоактивних відходів*}*; *{*Охорони державної таємниці*}*; *{*Дорогоцінними металами, Дорогоцінним камінням, Дорогоцінним камінням органогенного утворення, Напівдорогоцінним камінням*}*; *{*Оцінювання якості освіти, Проведення та перевірки результатів зовнішнього незалежного оцінювання*}*; державних *{*Спортивних заходів, Розважальних заходів*}*; *{*Надання медичної допомоги, Медичних послуг*}*	*{ВР};* *{ЗРВ}; {ОДТ};* *{ДМ, ДК, ДКОУ, НК};* *{ОЯО, ЗНО};* *{СЗ, РЗ};* *{МД, МП}*
Щодо розміщення {Р}	*{*Органів державної влади*}*, {Органів місцевого самоврядування*}*	*{ОДВ}, {ОМС}*

Таблиця 3

Група	*Елемент*	*Умовні позначення*
Уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, шкоди {УО}	*{*Від викликів, ризиків і загроз (кібератак), що можуть виникати щодо ОКІ*}*; *{*Здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення*)}*; *{*Соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства*)}*; *{*Економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих*)}*; *{*Природним ресурсам загальнодержавного значення*}*	*{КА};* *{УЗН};* *{УСС};* *{УЕ};* *{УПР}*
Масштабності негативних наслідків для держави {МНН}	*{*Вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів економіки*}*; *{*Призведуть до втрати унікальних національно значущих активів, систем і ресурсів*}*; *{*Матимуть тривалі наслідки для держави і позначаються на діяльності низки інших секторів*}*; *{*Від тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави*}*; *{*Від впливу на функціонування суміжних секторів критичної інфраструктури*}*; *{*Від завдання значної шкоди нормальним умовам життєдіяльності населення*}*	*{ВСО};* *{ВУА};* *{ТНД};* *{ТН};* *{ВСС};* *{ШНУ}*

4) За наслідками порушення сталого функціонування ОКІ, які можуть спричинити кібератаки [8, 10, 13, 15]: «{Виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону)}={Н1}; {Негативний вплив на стан енергетичної безпеки держави (регіону)}={Н2}; {Негативний вплив на стан економічної безпеки держави}={Н3}; {Негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі}={Н4}; {Негативний вплив на систему управління державою}={Н5}; {Негативний вплив на суспільно-політичну ситуацію в державі}={Н6}; {Негативний вплив на імідж держави}={Н7}; {Порушення сталого функціонування фінансової системи держави}={Н8}; {Порушення сталого функціонування транспортної інфраструктури держави (регіону)}={Н9}; {Порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав}={Н10}».

5) За методикою ідентифікації потенційно небезпечних об'єктів (табл. 4, 5) [18-22]:

Таблиця 4

Група	*Елемент*	*Умовні позначення*
За видом небезпеки {ВН}	*{*Бактеріологічна*}; {*Біологічна*}; {*Вибухопожежна*}; {*Гідродинамічна*}; {*Пожежна*}; {*Радіаційна*}; {*Фізична*}; {*Хімічна*}; {*Екологічна*}*	*{Б};{БЛ};{ВП}; {Г}; {П}; {Р}; {Ф}; {Х}; {Е}*
За класифікацією та кодом НС {КНС}	*{*Техногенні*}; {*Природні*}; {*Соціально-політичні*}; {*Воєнні*}*	*{Т}; {П}; {С-П}; {В}*
За рівнем можливої НС {РМНС}	*{*Державний*}; {*Регіональний*}; {*Місцевий*}; {*Об'єктовий (локальний)*}*	*{Д}; {Р};{М}; {О}*

Залежно від обсягів заподіяних наслідків, технічних і матеріальних ресурсів, необхідних для їх ліквідації, НС класифікується як: *{Д}; {Р}; {М}; {О}*. Для визначення відповідного рівня НС встановлюються критерії, що наведені у табл. 5 [19], де *РЗ* – розмір збитків, завданих уражальними чинниками джерела НС, розраховується відповідно до «Методики оцінки збитків від наслідків НС техногенного і природного характеру».

Таблиця 5

Рівень НС	*Територіальне поширення та обсяги технічних і матеріальних ресурсів, що необхідні для ліквідації наслідків НС*	*Кількість людей, які внаслідок дії уражальних чинників джерела НС загинули або постраждали, або нормальні умови життєдіяльності яких порушено (п.н.у.ж.)*	*РЗ (тис. мінімальних розмірів заробітної плати (м.р.з.п.))*
{Д}	територію інших держав; або територія двох чи більше регіонів України (Автономної Республіки Крим, областей, м. Києва та Севастополя), а для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують можливості цих регіонів, але не < 1% від обсягу видатків відповідних місцевих бюджетів (НС державного рівня за територіальним поширенням)	загинуло – [10; ∞[; постраждало – [300; ∞[; п.н.у.ж. – [50 000; ∞[(більш як на 3 доби)	[150; ∞[, який у інших випадках, передбачених актами законодавства, за своїми ознаками визначається як {Д}
		або загинуло – [5; 10[; постраждало – [100; 300[; п.н.у.ж. – [10 000; 50 000[(більш як на 3 доби)	[25; 150] (на час виникнення НС)
{Р}	територія двох чи більше районів (міст обласного значення) Автономної Республіки Крим, областей, а для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують можливості цих районів, але не < 1% обсягу видатків відповідних місцевих бюджетів (НС регіонального рівня за територіальним поширенням)	загинуло – [3; 4]; постраждало - [50; 100[; п.н.у.ж. – [1000; 10 000[;	[15; 25]
		(більш як на 3 доби)	[5; 15]
{М}	за межами території потенційно небезпечного об'єкта, загрожує довкіллю, сусіднім населеним пунктам, інженерним спорудам, а для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують власні можливості потенційно небезпечного об'єкта	загинуло - [1; 2]; постраждало – [20; 50[; п.н.у.ж. – [100; 1000[;	[2; 5]
		(більш як на 3 доби)	[0,5; 2]
{О}	визнається НС, яка не підпадає під названі вище визначення		

6) За категорією критичності [3, 13, 26]: {I категорія критичності – особливо (критично) важливі об'єкти}=*{ОВО}*; {II категорія критичності – життєво важливі об'єкти}=*{ЖВО}*; {III категорія критичності – важливі об'єкти}=*{ВО}*; {IV категорія критичності – необхідні об'єкти}=*{НО}*.

7) За класами наслідків (відповідальності) від категорії складності об'єкта (табл. 6) [23, 24]: {Незначні наслідки – I та II категорія складності}=*{СС-1}*: «Об'єкти промисловості, енергетики, транспорту і зв'язку, сільського господарства і переробки сільгосппродукції, що не віднесені до класів СС3 і СС2; громадські будівлі, об'єкти фізкультури та спорту, що не віднесені до класів СС3 і СС2, а також усі тимчасові об'єкти, мобільні будинки; об'єкти внутрішньовиробничих доріг, комунікацій і продуктопроводів; парники, теплиці; опори розподільної мережі низької напруги, освітлювальні опори» [23]; {Середні наслідки – III та IV категорія складності}=*{СС-2}*: «Об'єкти металургійної промисловості, важкого машинобудування, нафтохімії, суднобудування, оборонної промисловості (доменні і мартенівські цехи, складальні корпуси, високі димові труби тощо); копри, машинні відділення добувних машин; об'єкти гідро- і теплоенергетики потужністю <1,0 млн. кВт, розподільні системи основних електромереж високої напруги (включаючи опори ліній електропередачі і відкритих розподільних пристроїв); ємкості для нафти і нафтопродуктів; шляхові полотна магістральних автодоріг, злітно-посадкові смуги, мости і тунелі протяжністю <1000 м, канатні дороги, вокзали, аеровокзали, вертолітні станції; магістральні трубопроводи; великі готелі, гуртожитки; об'єкти водопроводу і каналізації (включаючи водонапірні башти, очисні споруди, водозабори) промислових підприємств і населених пунктів; будівлі видовищних і спортивних підприємств, підприємств торгівлі, громадського харчування, служби побуту, установи охорони здоров'я; будівлі і споруди центральних складів для забезпечення життєвих потреб населення, склади особливо цінного устаткування і матеріалів, військові склади; житлові, громадські або бага-

тофункціональні будівлі заввишки до 100 м.» [23]; {Значні наслідки – V категорія складності}={*CC-3*}: «Об'єкти нафто- і газодобувної, газопереробної, металургійної, хімічної та інших галузей промисловості, обладнані пожежо- і вибухонебезпечними ємкостями і сховищами рідкого палива, газу і газопродуктів, особливо при їх зберіганні під тиском (технологічні трубопроводи, апарати, котли, газгольдери, ізотермічні резервуари ємністю >10 тис. кубометрів, резервуари для зберігання нафти та нафтопродуктів ємністю >30 тис. кубометрів, посудини високого тиску тощо); об'єкти хімічної, нафтохімічної, біотехнологічної, оборонної та інших галузей, що пов'язані з використанням, переробкою, виготовленням і зберіганням хімічно токсичних, вибухо- і пожежонебезпечних речовин і промислових вибухових матеріалів, біологічно небезпечних речовин тощо; об'єкти вугільної і гірничорудної промисловості, небезпечні щодо пожежі, вибуху і газу відповідно до класифікації Держнаглядохоронпраці; будівлі головних вентиляційних систем на копальнях і рудниках; об'єкти атомної енергетики (АЕС, АЕТС, АСТ), включаючи сховища і заводи з переробки ядерного палива і радіоактивних відходів, а також інші радіаційне небезпечні об'єкти за класифікацією Держатомнагляду; об'єкти гідро- і теплоенергетики (ГЕС, ГРЕС, ТЕС, ТЕЦ, ГАЕС) потужністю >1,0 млн. кВт; мости і тунелі на дорогах вищої категорії, або протяжністю >1000 м чи прогоном >300 м; стаціонарні споруди знаків навігаційної обстановки; шлюзи і основні портові споруди на водних шляхах 1-го і 2-го класів ДСТУ Б В.2.3-1; будівлі і споруди крупних залізничних вокзалів і аеровокзалів; магістральні трубопроводи діаметром >1000 мм, або з робочим тиском >2,5 МПа, а також ділянки магістральних трубопроводів меншого діаметра і з меншим робочим тиском у місцях переходів через водні перешкоди, залізничні та автомобільні дороги; гідротехнічні споруди меліоративних систем із площею зрошення і осушення >300 тис. га і водоймищ об'ємом >1 кубічний кілометр; крупні елеватори і зерносховища, млинарські комбінати; житлові, громадські або багатофункціональні будівлі заввишки >100 м; будівлі основних музеїв, державних архівів, сховищ національних історичних і культурних цінностей; видовищні об'єкти з масовим перебуванням людей (стадіони, театри, кінозали, цирки, виставкові приміщення тощо); будівлі університетів, інститутів, шкіл, дошкільних закладів тощо; великі лікарні та інші заклади охорони здоров'я; універсами та інші великі торговельні підприємства; об'єкти життєзабезпечення великих районів міської забудови і промислових територій; великі об'єкти захисно-запобіжного характеру (протиселеві, протизсувні, протилавинні споруди, захисні дамби тощо)» [23].

Таблиця 6

Характеристики можливих наслідків від відмови будівлі або споруди за класами наслідків (відповідальності) [24]

Клас наслідків (відповідальності) будівлі або споруди	*Характеристики можливих наслідків від відмови будівлі або споруди*					
	Можлива небезпека для здоров'я і життя людей (кількість осіб)			*Обсяг можливого економічного збитку (м.р.з.п.)*	*Втрата об'єктів культурної спадщини (за рівнем НС)*	*Припинення функціонування комунікацій транспорту, зв'язку, енергетики, інших інженерних мереж (рівень НС)*
	які постійно перебувають на об'єкті	*які періодично перебувають на об'єкті*	*які перебувають поза об'єктом*			
{СС-3}	[400; ∞[	[1000; ∞[	[50 000; ∞[	[50 000; ∞[	*{Н}*	*{Д}*
{СС-2}	[50, 400[	[100; 1000[	[100, 50 000[	[2500; 50 000[	*{М}; {О}*	*{Р}; {М}*
{СС-1}	[0; 50[	[0; 100[	[0; 100[	[0; 2500[	–	–

8) За наявністю ОКІІ [12, 14, 24]: {Комунікаційна система}={КС}; {Технологічна система}=*{ТС}*; {Інформаційні системи}=*{ІС}*; {Інформаційно-телекомунікаційні системи та мережі}=*{ІТС}*; {Автоматизовані системи управління технологічним процесом}=*{АСУ}*.

9) За ознаками ідентифікації об'єктів підвищеної небезпеки (табл. 7) [20-22].

10) За видом інформації, що обробляється (табл. 8) [12, 14, 15].

Таблиця 7

Група	*Елемент*	*Умовні позначення*
За категорією наявних небезпечних речовин {КНР}	*{*Горючі (займисті) гази*}*; *{*Горючі рідини*}*; *{*Горючі рідини, перегріті під тиском*}*; *{*Вибухові речовини*}*; *{*Речовини-окисники*}*; *{*Високотоксичні та токсичні речовини*}*; *{*Речовини, які становлять небезпеку для довкілля (високотоксичні для водних організмів)*}*	*{ГГ}; {ГР}; {ГПТ}; {ВР};{Р-О}; {ВТР}; {РНД}*
За видами та впливом уражальних факторів аварій, що можуть статися виходячи з властивостей небезпечних речовин {УФА}	*{*Група 1 (вибух)*}*; *{*Група 2 (пожежа)*}*; *{*Група 3 (шкідливі для людей і довкілля)*}*	*{Г1}; {Г2}; {Г3}*

Таблиця 8

Група	*Елемент*	*Умовні позначення*
Національні електронні інформаційні ресурси {НЕІР}	*{*Публічна інформацію*}*; *{*Державні інформаційні ресурси*}*; *{*Інша інформація, призначена для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави*}*	*{ПІ}; {ДІР}; {ІІ}*
Інформація з обмеженим доступом {ІзОД}	*{*Конфіденційна інформація (у т.ч. персональні дані)*}*; *{*Службова інформація*}*; *{*Таємна інформація*}*	*{КІ}; {СІ}; {ТІ}*

Далі, на основі проведеного аналізу та запропонованого переліку узагальнених критеріїв віднесення об'єктів до ОКІД сформуємо відповідну базову множину:

$$\mathbf{МК} = \{\bigcup_{i=1}^{n} \mathbf{МК}_i\} = \{\mathbf{МК}_1, \mathbf{МК}_2, ..., \mathbf{МК}_n\}, \quad (1)$$

де $\mathbf{МК}_i \subseteq \mathbf{МК}$ $(i = \overline{1,n})$ – множина, що відображає *i*-й критерій, *n* – кількість цих критеріїв.

Наприклад, з урахуванням низки вищенаведених ознак, при $n = 10$, $(i = \overline{1,10})$ відповідно до [1-26], формула (1) набуде вигляду:

$$\mathbf{МК} = \{\bigcup_{i=1}^{n} \mathbf{МК}_i\} = \{\mathbf{МК}_1, \mathbf{МК}_2, ..., \mathbf{МК}_{10}\} =$$

$$= \{\boldsymbol{СД}, \boldsymbol{ОВО}, \boldsymbol{ВФП}, \boldsymbol{НК}, \boldsymbol{ПНО}, \boldsymbol{КК}, \boldsymbol{КН}, \boldsymbol{ОКІІ}, \boldsymbol{ОПН}, \boldsymbol{ВІ}\},$$

де $\mathbf{МК}_1 = \boldsymbol{СД}$ = «За сферою діяльності та надання послуг у секторі критичної інфраструктури», $\mathbf{МК}_2 = \boldsymbol{ОВО}$ = «За критеріями включення до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг», $\mathbf{МК}_3 = \boldsymbol{ВФП}$ = «За сукупністю критеріїв, що визначають їх важливість для реалізації життєво важливих функцій та послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення.

Висновок

Сформовано перелік узагальнених критеріїв віднесення об'єктів до критичної інфраструктури держави у вигляді базової множини, яка інтегрує одинадцять ознак з можливістю подальшого розширення.

Даний перелік містить критерії, які визначають належність певного об'єкту не тільки до об'єктів критичної інфраструктури держави за методикою їх віднесення, але й до інших важливих для країни об'єктів, визначених відповідними державними реєстрами.

Цю базову множину можна використати для визначення пріоритетності кіберзахисту об'єктів критичної інформаційної інфраструктури, наприклад, інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Література

[1]. A. Korchenko, Y. Dreis, O. Romanenko, "Analysis problems in the field of state's critical infrastructure", *Projekt interdyscyplinarny projektem XXI wieku: Monografia. Tom 1*. – Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2017. – pp. 397 - 402.

[2]. "*Зелена книга з питань захисту критичної інфраструктури в Україні*", Д. Бірюков, С. Кондратов, О. Суходоля. – К: НІСД, С. 176, 2016. URL: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf

[3]. *Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп.* / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.

[4]. О. Корченко, Ю. Дрейс, О. Романенко, В. Бичков, "Модель класифікатора об'єктів критичної інформаційної інфраструктури держави", *Захист інформації*. – 2018. – Т. 20, № 1. – С. 5-11.

[5]. О. Корченко, Ю. Дрейс, О. Романенко, "Класифікація об'єктів критичної інформаційної інфраструктури держави", *зб. тез наук. доп. наук.-практ. конф.* (Київ, 30 березня 2018 р.). – Київ: Нац.акад.СБУ, 2018. – 408 с. – С. 95-98.

[6]. О. Корченко, Ю. Дрейс, О. Романенко, "Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури", *«Актуальні проблеми забезпечення кібербезпеки та захисту інформації»*, тези доповідей учасників IV Міжнародної науково-практичної конференції, Закарпатська обл., с. Верхнє Студене, 21-24 лютого 2018 р. – К: Ви-во Європейського університету, 2018. – С. 81-86.

[7]. С. Гнатюк, В. Сидоренко, Н. Сєйлова, "Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави", *Безпека інформації*, Том 23, № 2(2017 р). – С. 87–91.

[8]. О. Корченко, Ю. Дрейс, О. Романенко, "Критична інформаційна інфраструктура України: терміни, сектори і наслідки", *Захист інформації*. – 2017. – Т. 19, № 4. – С. 303-309.

[9]. Y. Dreis, M. Roshchuk, O. Romanenko, "Sectors of Critical Informational Infrastructure", *тези доповідей учасників IV Міжнародної науково-практичної конференції*, Закарпатська обл., Міжгірський р-н, с. Верхнє Студене, 21-24 лютого 2018 р. – К: Ви-во Європейського університету, 2018. – С.141-143.

[10]. Ю. Дрейс, "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", *Захист інформації*. – 2017. – Т. 19, № 3. – С. 214-222.

[11]. Ю. Дрейс, О. Романенко, "Розширення базової термінології у сфері захисту критичної інформаційної інфраструктури держави", *Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті: матеріали всеукраїнської науково-практичної інтернет-конференції*, 16–17 листопада 2017, Кропивницький: ЦНТУ, 2017. – С. 185–187.

[12]. "*Про основні засади забезпечення кібербезпеки України*", Верховна Рада України, Закон України від 05.10.2017р. URL: http://zakon2.rada.gov.ua /laws/show /2163-19.

[13]. "*Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури*", проект Постанови Кабінету Міністрів України (18.05.2018), Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс]. Режим доступу: http://195.78.68. 84/dsszzi/control/uk/publish/article?art_id=290126&cat_id =38837.

[14]. "*Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури*", Постанова №518 від 19.06.2019, Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8.

[15]. "*Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави*", Кабінет Міністрів

України; Постанова, Порядок від 23.08.2016 № 563. URL: http://zakon5.rada.gov.ua/laws/show/563-2016-п.

[16]. "*Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні. Аналітична записка*", Національний інститут стратегічних досліджень, відділ екологічної та техногенної безпеки (Д.С. Бірюков). URL: http://old2.niss.gov.ua/ articles/1477/.

[17]. "*Про затвердження Критеріїв, відповідно до яких об'єкти включаються до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг*", Міністерство внутрішніх справ, Наказ від 01.09. 2015 № 1053. URL: https://zakon.rada.gov.ua/laws/ show/z1124-15.

[18]. "*Про критичну інфраструктуру та її захист*", Міністерство економічного розвитку і торгівлі України, Проект Закону України. URL: http://www. me.gov.ua/ Documents/Download?id=634a8762-3d1a-45ac-b0df-be56 a4f7d9d1.

[19]. "*Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями*", Кабінет Міністрів України; Постанова, Порядок від 24.03.2004 № 368 (редакція від 11.06.2013). URL: https://zakon.rada.gov. ua/laws/show/368-2004-%D0%BF.

[20]. "*Про затвердження Методики ідентифікації потенційно небезпечних об'єктів*", Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Наказ від 23.02.2006 № 98. URL: https://zakon.rada.gov. ua/laws/show/z0286-06.

[21]. "Про об'єкти підвищеної небезпеки ", Верховна Рада України, Закон України від 18.01.2001р. №2245-III. URL: https://zakon.rada.gov.ua/laws/show/ 2245-14.

[22]. "*Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки*", Кабінет Міністрів України; Постанова від 11.07.2002 № 956. URL: https:// zakon2.rada.gov.ua/laws/show/956-2002-%D0% BF.

[23]. "*Про регулювання містобудівної діяльності*", Верховна Рада України, Закон України від 17.02.2011 р. URL: https://zakon.rada.gov.ua/laws/show /3038-17.

[24]. "*О безопасности критической информационной инфраструктуры Российской Федерации*", Федеральный закон от 26 июля 2017 г. N 187-ФЗ. URL: http://ivo. garant.ru/#/document/71730198/paragraph/1:0.

[25]. A. Korchenko, V. Hrebenuik, Y. Dreis, A. Hrebenuik, O. Gavrylenko, Criteria for assigning objects to critical infrastructure of Ukraine, «*Przetwarzanie, transmisja i bezpieczenstwo informacij»: Monografia, Tom* 2, Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2019. – С. 189-196.

[26]. "*Деякі питання об'єктів критичної інфраструктури*", Кабінет Міністрів України; Постанова від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/ laws/show/1109-2020-%D0%BF#n91.

УДК 004.056:007.2

Дрейс Ю.А., Деркач Л.В. Базовое множество обобщенных критериев отнесения объектов к критической инфраструктуры государства.

Аннотация. *Отсутствие реестров объектов критической инфраструктуры государства и их информационно-телекоммуникационных систем приводит к неопределенности в количестве необходимых ресурсов для обеспечения их защиты от возможных кибератак. Учитывая ограниченность таких ресурсов, важным и актуальным научно-практической задачей является определение полноты и границ приоритетности киберзащиты указанных объектов. Формирование таких реестров происходит по методике отнесения объектов к критической инфраструктуры государства, основанной в т.ч. на благоприятных условиях, которые будут определять принадлежность определенного объекта к такому, что является критическим для государства. Проведенный анализ существующих критериев отнесения объектов к критической инфраструктуры государства, показывает, что в Украине существует ряд других критериев (и которые следует также учитывать), задействованных в формировании реестров важных для государства объектов, например, «Государственный реестр потенциально опасных объектов». Итак, предлагается сформировать перечень таких обобщенных критериев отнесения объектов к критической инфраструктуры государства в виде базовой множества, которая интегрирует десять признаков с возможностью дальнейшего расширения. Такое множество можно использовать для определения приоритетности киберзащиты информационно-телекоммуникационных систем (объектов критической информационной инфраструктуры) объектов критической инфраструктуры государства.*

Ключевые слова: *объекты критической инфраструктуры государства, множество критериев критичности, критическая информационная инфраструктура.*

Y. Dreis, L. Derkach, Basic set of generalized criteria for assigning objects to the critical infrastructure of state.

Abstract. *The lack of registers of critical infrastructure of the state and their information and telecommunication systems leads to uncertainty in the amount of resources needed to protect them from possible cyberattacks. Given the limitations of such resources, an important and relevant scientific and practical task is to determine the completeness and priority of cyber protection of these objects. The formation of such registers is based on the method of assigning objects to the critical infrastructure of the state, including on the relevant criteria that will determine the affiliation of a particular object to one that is critical to the state. The analysis of the existing criteria for classifying objects as critical infrastructure of the state shows that in Ukraine there are a number of other criteria (and which should also be taken into account) involved in the formation of registers of important objects for the state, such as "State Register of Potentially Dangerous Objects". Therefore, it is proposed to form a list of such generalized criteria for classifying objects as critical infrastructure of the state in the form of a basic set, which integrates ten features with the possibility of further expansion. This set can be used to determine the priority*

of cyber protection of information and telecommunications systems (critical information infrastructure facilities) of critical infrastructure facilities of the state.
Key words: *objects of critical infrastructure of the state, set of criteria of criticality, critical information infrastructure.*

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, старший науковий співробітник Національної академії СБ України.
Дрейс Юрий Александрович, кандидат технических наук, доцент, старший научный сотрудник Национальной академии СБ Украины.
Yurii Dreis, PhD in Eng. (Information security), Associate Professor, Senior Research Fellow of the National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Деркач Леонід Васильович, старший науковий співробітник Національної академії СБ України.
Деркач Леонид Васильевич, старший научный сотрудник Национальной академии СБ Украины.
Leonid Derkach, General of the Army of Ukraine, Senior Research Fellow of the National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Отримано *15 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY&PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.26.15574

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ЗА ДОПОМОГОЮ ПРИМАНОК У ХМАРНОМУ СЕРЕДОВИЩІ

Опірський Іван, Сусукайло Віталій, Василишин Святослав

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
Orcid ID:0000-0002-8461-8996.

ВАСИЛИШИН Святослав Ігорович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 1995 рік, м. Львів, Львівська область, Україна.
Наукові інтереси: засоби захисту інформації в гібридних та кібер війнах, білий хакінг
E-mail: swat2244@gmail.com.
Orcid ID:0000-0003-1944-2979.

СУСУКАЙЛО Віталій Андрійович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 1995 рік, м. Львів, Львівська область, Україна.
Наукові інтереси: системи менеджменту інформаційної безпеки, системи дослідження кіберзлочинів.
E-mail: vitalii.susukailo@gmail.com.
Orcid ID:0000-0003-4431-9964.

Анотація. *Хмарні технології дедалі частіше використовуються. Хоча хмарне середовище може дати організаціям свободу експериментувати та масштабувати ресурси, воно також збільшує поверхню атаки. Ця стаття досліджує можливості приманок в хмарних середовищах. Аналізує проблему розслідування кіберзлочинів у хмарах. Визначає та вивчає відповідні технології, що використовуються фахівцями з кібербезпеки під час розслідування кіберзлочинів. Визначає переваги використання приманок у хмарній інфраструктурі. Для хмарних середовищ загрозою номер один є порушення даних. Порушення можуть завдати великої репутаційної та фінансової шкоди. Вони можуть потенційно призвести до втрати інтелектуальної власності та значних юридичних зобов'язань. Неадекватне управління доступом, у хмарному середовищі, загроза, що може призвести до компрометації хмарної системи. Щоб уникнути цієї загрози, клієнти хмари повинні захищати облікові дані, забезпечувати автоматичне обертання криптографічних ключів, паролів та сертифікатів, забезпечувати масштабованість, вимагати від адміністраторів хмарних служб використання багатофакторної автентифікації, визначати політику паролів для площини управління та кожної служби, розгорнутої в хмарі. Визначено, що рекомендується використовувати мережу "приманок" у хмарній службі як послугу (HaaS). Це дозволяє зменшити початкові та експлуатаційні витрати на підтримку Інфраструктури, підвищити ефективність розгортання системи та забезпечити можливість віддаленого управління.*

Ключові слова: *приманка, хмарне середовище, хмарна інфраструктура, кіберзлочинність, веб-служби Amazon, хмарна платформа Azure, IaaS, PaaS, SaaS.*

Вступ

Хмарні технології дедалі частіше використовуються. Хоча хмарне середовище може дати організаціям свободу експериментувати та масштабувати ресурси, воно також збільшує поверхню атаки.

Хмарна безпека є спільною відповідальністю хмарного провайдера та хмарного замовника. Залежно від моделі хмарного сервісу, обов'язки щодо захисту інформації повинні бути адекватно визначені та задокументовані.

Для моделей SaaS та PaaS постачальник відповідає за засоби контролю рівня інфраструктури, такі як виправлення послуг та операційної системи, управління уразливістю, зміцнення гіпервізора, фізичну безпеку центру обробки даних тощо.

Але в той же час це не означає, що клієнт не несе відповідальності за засоби захисту інформації. Клієнти хмарних служб, які використовують сервіси SaaS та PaaS, повинні дотримуватися рекомендацій щодо посилення постачальників та найкращих практик безпеки для програм чи служб, якими вони користуються.

Також необхідно регулярно проводити оцінку безпеки постачальника для оцінки засобів контролю, що надаються SaaS або постачальником послуг PaaS, щоб переконатися, що програма забезпечує відповідний контроль безпеки та відповідає вимогам міжнародних законів та норм.

Для Інфраструктури як моделі послуги, клієнт хмари відповідає за конфігурацію операційної системи, масштабування ресурсів, програмне управління мережами та підтримку рівня інфраструктури, крім фізичної безпеки, гіпервізорів, управління мережею та віртуальними машинами.

Це означає, що існує більше засобів контролю, які слід визначити для IaaS, таких як моніторинг безпеки, управління вразливістю, управління інцидентами, зміцнення операційної системи тощо. Це також відповідальність клієнта хмари за виявлення та відповідь на загрози хмарної безпеки та забезпечення належного захисту від кіберзлочинів. Існує безліч інструментів та технологій кібербезпеки, що надаються постачальниками хмарних послуг, які можуть виявити та запобігти кіберзлочинам. Тим не менш, у цій статті основна увага буде приділена надійним та зрозумілим рішенням для розслідування інцидентів у IaaS.

Загрози кібербезпеки для хмарних середовищ. Для хмарних середовищ загрозою номер один є порушення даних. Порушення можуть завдати великої репутаційної та фінансової шкоди. Вони можуть потенційно призвести до втрати інтелектуальної власності (ІВ) та значних юридичних зобов'язань. Неадекватне управління доступом, у хмарному середовищі, загроза, що може призвести до компрометації хмарної системи.

Щоб уникнути цієї загрози, клієнти хмари повинні захищати облікові дані, забезпечувати автоматичне обертання криптографічних ключів, паролів та сертифікатів, забезпечувати масштабованість, вимагати від адміністраторів хмарних служб використання багатофакторної автентифікації, визначати політику паролів для площини управління та кожної служби, розгорнутої в хмарі.

Ще однією поширеною загрозою хмарної безпеки є незахищені інтерфейси та API. API та користувальницькі інтерфейси часто є найбільш відкритими частинами системи, і це заохочує безпеку шляхом дизайнерського підходу до їх побудови.

Для забезпечення захисту від цих загроз компанія Cloud Security Alliance запропонувала такі засоби контролю:

– Повинні бути встановлені найкращі практики безпеки API, такі як нагляд за такими предметами, як інвентаризація, тестування, аудит та захист від ненормальної діяльності.

– Ключі API слід захищати, а також уникати повторного використання будь-якого ключа.

– Рекомендується використовувати відкриту структуру API, таку як Open Cloud Computing Interface (OCCI) або Cloud Infrastructure Management Interface (CIMI).

Відсутність архітектури та стратегії хмарної безпеки - ще одна критична загроза, яку слід враховувати при оцінці ризиків хмарних служб.

Архітектура безпеки повинна узгоджуватися з бізнес-цілями та завданнями, моделювання загроз слід проводити регулярно, а також слід забезпечувати постійний моніторинг для кожного типу моделі хмарних служб.

Ці засоби управління можуть допомогти організаціям забезпечити безпечну архітектуру для хмарної інфраструктури.

Зловмисники використовують законні хмарні сервіси для підтримки своєї діяльності. Хакери можуть використовувати популярний сервіс для зберігання зловмисного програмного забезпечення на таких веб-сайтах, як GitHub, тому для хмарних клієнтів дуже важливо контролювати вміст, що використовується їхнім хмарним рішенням.

Поширені локальні загрози застосовні до хмарних середовищ, такі як DDoS-атаки, видобуток цифрових валют, грубі атаки для викрадення облікових даних, використання вразливостей застарілого програмного забезпечення тощо.

Ці загрози повинні оцінюватися та пом'якшуватися клієнтами хмарних служб, щоб уникнути потенційної злочинності в хмарі, що спричинить підприємницьку шкоду.

Розслідування злочинів у хмарній безпеці за допомогою хмарного рішення безпеки. Розслідування злочинів у хмарній безпеці може здійснюватися за допомогою інструментів, наданих постачальником хмарних послуг.

Існує безліч технологій моніторингу, виявлення та реагування на безпеку, які можна використовувати для аналізу злочинів у хмарній безпеці та їх запобігання, а також сторонніх технологій, які можна використовувати в хмарному середовищі, таких як Splunk, стек ELK, LogRhythm тощо.

Але найпопулярніші постачальники хмарних послуг, такі як Amazon Web Services та Azure, мають вбудовані рішення для кібербезпеки.

Одним із рішень, яке можна використовувати для розслідування злочинів у хмарній безпеці, є Azure Log Analytics, технологія управління хмарними подіями Azure і частина Центру безпеки Azure.

Log Analytics є частиною загального рішення моніторингу Microsoft Azure. Log Analytics відстежує хмарне та локальне середовища для підтримки як кінцевих точок, так і доступності та продуктивності корпоративних служб. Azure Log Analytics як інструмент для дослідження подій у хмарному середовищі Azure може виконувати такі функції:

– Збір інформації - детальних поточних показників та журналів - із ресурсів Azure та місцевої інфраструктури.

– Візуалізація - вбудовані інформаційні панелі для візуалізації, які допоможуть швидко зрозуміти, що сталося.

– Аналіз - аналіз програм та інфраструктури.

– Відповідь - автоматична реакція на випадки.

– Інтеграція - використання 20+ партнерських інтеграцій та відкритої структури з API та SDK.

Azure Log Analytics може аналізувати будь-які завантажені в неї дані. Ця функціональність забезпечує аналіз системних та службових подій без обмежень, що дуже важливо для аналізу даних з кількох джерел під час розслідування інцидентів у хмарній безпеці. Також можна створити власні пошуки та правила оповіщення для автоматизації пошуку погроз та процесів розслідування інцидентів. Також усі журнали, що зберігаються на платформі Azure Log Analytics, можуть використовуватися для подальшої криміналістики.

Amazon Web Services мають власні засоби контролю безпеки, такі як Amazon Guard Duty та AWS Cloud Trail. Amazon представляє AWS CloudTrail як технологію, яка забезпечує історію подій активності облікового запису, включаючи дії, вжиті через площину управління, SDK AWS, інструменти CLI та інші служби Amazon. Історія викликів API спрощує аналіз безпеки, відстеження змін та усунення несправностей. Крім того, CloudTrail можна використовувати для виявлення незвичної активності в облікових записах Amazon. Amazon GuardDuty - це служба виявлення загроз, яка контролює зловмисні дії та несанкціоновану поведінку для захисту хмарних облікових записів, робочих навантажень та даних, що зберігаються в Amazon S3.

Служба використовує машинне навчання, виявлення аномалій та інтегровану інформацію про загрози для виявлення та визначення пріоритетів потенційних загроз. GuardDuty може аналізувати кілька подій у кількох джерелах даних AWS, таких як журнали подій AWS CloudTrail, журнали потоків Amazon VPC та журнали DNS. Обидва ці сервіси Amazon GuardDuty та Cloud Trail повинні ефективно розслідувати злочини хмарної безпеки в Amazon Web Services.Вбудовані технології моніторингу хмарної безпеки можна ефективно використовувати з іншими рішеннями безпеки для запобігання та виявлення кіберзлочинів хмарної безпеки.

Типи пасток, поведінка та ефективність у хмарному середовищі. Пастка принципово відрізняється від усіх подій у галузі безпеки. Як правило, усі продукти на цьому ринку розроблені для вирішення суворо визначеної функції (неважливо, чи йдеться про апаратне чи програмне забезпечення): брандмауер вирішує завдання обмеження доступу з однієї мережі в іншу на різних рівнях, SSH Послуга призначена для зашифрованого доступу до ресурсів операційної системи тощо.

Технологія приманки не призначена для вирішення конкретної проблеми, а представляє цілу філософію - гнучка, настроювана відповідно до мети. Як можна здогадатися, це не формалізований продукт чи технологія, а такий собі інструмент, щось на зразок мікроскопа в руках біолога.

Пастка надає фахівцям із безпеки значні переваги. Перш за все, це збір необхідної інформації, часто містить цінну інформацію. Розгортання та експлуатація приманок не представляє особливих труднощів, а інструменти пастки, як правило, не вимагають системних ресурсів.

Особливу увагу слід приділити встановленню та експлуатації пасток. Як правило, весь спектр заходів зводиться до "встановлення та очікування". Найпоширеніший випадок - із виділеним сервером під контролем фахівців.

Сьогодні існує багато фальшивих програм, які створюють враження справжніх, але не так, їх головне завдання - записати весь обмін. Перевага пастки полягає в тому, що копію програмного забезпечення можна зробити на морально застарілому сервері, який не може впоратися з типовими обчислювальними завданнями електронного бізнесу.

Залежно від рівня складності та його можливостей їх можна класифікувати на три групи: слабкі, середні та сильні рівні взаємодії:

1. Низький рівень: простий у використанні та дуже надійний. Вони імітують лише частину служб, і зловмисник буде обмежений у взаємодії з ними. Наприклад, вони можуть імітувати систему UNIX, на якій запущено telnet. Такі системи призначені для самих початківців зломщиків. Ризик використання пасток низького рівня мінімальний, але він є. Це пов'язано з тим, що саме програмне забезпечення теж є програмою; отже, воно може бути вразливим. Якщо його можна обійти, зловмисник отримає доступ до решти вузлів мережі. Сильною стороною цих найпростіших пасток у тому, що вони прості самі по собі. Відомо, що чим простіші, тим надійніші, тому ці програми мінімізують ризик, пов'язаний з можливою поломкою самої приманки і наступною поломкою системи.

2. Приманки середнього рівня надають більше можливостей для реконструкції зломщика, більш складного і, отже, більш вразливого. Наприклад, така система може моделювати більш складні веб-сервери, які можуть реагувати на нестандартні команди та мати більш досконалу систему логування. В UNIX ви можете використовувати можливості команд chroot, а в Windows - віртуальні машини VMWare. Таким чином, розширюється середовище зловмисника (тобто він зможе взаємодіяти не тільки з «підробленими» службами, але і з «підробленою» ОС), і це дасть більше можливостей для логування. Але такий підхід також створить більше проблем.

3. Високий рівень: надає максимум інформації про нападника і є максимально складними та небезпечними. Вони дають зловмиснику доступ до реальної системи, яка нічого не робить і не підключена до інших систем. Структура такої приманки найчастіше така: вузол приманки, мережевий датчик та сховище інформації. Такий вузол може бути розташований у мережі за брандмауером, і тоді фактичний контроль лежить на брандмауері. Якщо вузол приманки неправильно налаштований або трапляються якісь інші непередбачені ситуації, зловмисник зможе отримати доступ до мережі.

Одним з недоліків такого рішення може бути складність його реалізації та відносна вартість підтримки. Згідно з останніми дослідженнями загалом системи приманки мають високу оцінку та широко використовуються в різних організаціях.

Ідея пастки представлена в більш широкому розумінні - на рівні всієї мережі. Це певний вид приманки; однак така система складається не з одного комп'ютера або активного мережевого пристрою, а з цілої мережі.

Пастка - інструмент розслідування. Найцінніша причина розслідування кіберзлочинів через пастки у мережі - це інформація, яку вона надає; те, чого не може забезпечити жодна система виявлення та запобігання вторгнень.

Озброївшись інформацією та попередженнями, які вони реєструють, адміністратори мережі дізнаються про типи атак, на які вони націлені, та мають попередні знання, щоб зрозуміти, що їм потрібно зробити для посилення захисту.

Таблиця порівняння пасток показує відмінності між постачальниками в таблиці 1.

Існує два типи приманок:

1. Підприємницька «пастка» - це «пастка», яка розміщена у виробничому середовищі та служить інструментом для розслідування атак з метою використання знань для подальшого посилення безпеки мережі.

2. Дослідницька пастка - це «пастка», яка використовується дослідниками з надією вивчити методології нападу та інші характеристики, такі як мотиви нападу. Потім, наприклад, використовуючи знання для створення захисних рішень (антивірусів, антивірусів тощо), які можуть запобігти подібним атакам у майбутньому. Типи даних, які збирають (або подібне) зловмисники "пасток", можуть включати, але не обмежуючись ними:

1. Імена користувачів, ролі та привілеї, якими користуються зловмисники;

2. IP-адреси мережі або хоста, що використовуються для атаки;

3. Які дані досягнуті, модифіковані чи виключені;

4. Фактичні натискання клавіш набирання тексту, дозволяючи адміністраторам точно бачити, що вони роблять.

Пастки також допомагають утримувати увагу хакерів відверненою від головної мережі, запобігаючи повному обсягу атак, поки адміністратори не будуть готові вжити належних контрзаходів. Нарешті, ми повинні згадати плюси та мінуси використання пасток у вашій мережі.

Плюс: це недорогий захід безпеки, який може надати цінну інформацію про ваших зловмисників.

Мінус: не легко встановити та налаштувати, і божевільно пробувати це, не маючи під рукою експерта; це може дати негативні наслідки та піддати мережу найгіршим атакам.

Однак само собою зрозуміло, що приманки - це, мабуть, найкращий спосіб зловити хакера або атакувати, як це трапляється.

Це дозволяє адміністраторам пройти весь процес крок за кроком, стежачи за всім у реальному часі з кожним попередженням.

Таблиця 1

Порівняння пасток

Постачальник /	**Платформа**	**TrapX DeceptionGrid**	**Платформа**
Фейкові платформи ОС		Windows, Linux	Windows,Linux
Поетапне виявлення атаки	Активний інте-	Активний інтелект	Активний інтелект
Виявлення C&C	–	+	–
Виявлення MITM	–	+	–
Емульовані пастки	+	+	+
Промислові приманки	+	+	–
Інтеграція NAC	+	+	–
Повні пастки ОС	+	+	+
Інтеграція SIEM	+	+	+
Інтеграція кінцевої точки	+	+	+
EDR	+	+	+
Активна Директорія	+	+	+
Вбудована кореляція	+	+	+
Інтеграція пісочниці	–	+	–
База даних	–	+	+
POS	–	+	–
ATM	–	+	–
SCADA	+	+	+
IoT	+	+	+
Хмари	невідомо	AWS/Azure/OpenStack	–
Використання клієнтських зображень	+	+	+
Відкритий API для інтеграції	+	+	+
Виявлення ботнетів	–	+	Дорожня карта
Автоматичний аналіз коду	–	+	–
Конструктор пастки	–	+	+
Передача стану API	–	+	+
Колекція криміналістики	+	–	+
Роздача приманок справжнім господарям	+	–	+
Механізм створення приманки при AD	–	–	+
Інтеграція з системами оркестрації контейнерів	–	невідомо	+

Не потрібно глибокого втручання в мережеву інфра-	+	–	+
Можливість повного адміністративного доступу в ОС	+	–	+

Висновок

Основним завданням, яке вирішують фахівці з інформаційної безпеки на об'єктах інформаційно-телекомунікаційної інфраструктури, є збір інформації для запобігання атакам на об'єкти інформації, що захищаються. Раніше збір інформації проводився після виникнення інциденту з інформаційною безпекою, потім на основі отриманих даних були випущені "латки" та "латання дірок" в системі безпеки.

Єдиною інформацією, якою мали у своєму розпорядженні спеціалісти з інформаційної безпеки, була інформація, залишена в скомпрометованій системі. Як правило, цієї інформації дуже мало, і її не вистачає для запобігання подальшій загрозі безпеці захищених інформаційних ресурсів. Використання мережевих точок доступу для виявлення атак на захищені інформаційні ресурси дозволить зібрати якомога більше інформації про саму атаку та про цілі зловмисників, а також запобігти несанкціонованому доступу до захищених інформаційних ресурсів. Мережева пастка повинна працювати в стелс-режимі, щоб зловмисник не знав про її присутність.

В даний час існує стійка тенденція передачі обчислювальних потужностей хмарній інфраструктурі. Технологія хмарних обчислень - це технологія та бізнес наступного покоління.

Постачальники хмарних послуг повинні забезпечувати безпеку послуг, які вони надають. Підприємства прагнуть перенести свою інформаційну інфраструктуру на хмарні сервіси, але більшість з них не можуть дозволити собі загрози інформаційної безпеки.

Здебільшого існуючі хмарні служби пропонують стандартний набір засобів захисту інформації, таких як різні брандмауери, використання різних методів автентифікації, системи виявлення атак на основі аналізу підписів тощо.

Хмарні служби, в порівнянні з класичними інформаційними системами, є більш вразливими з точки зору шкоди.

У хмарному середовищі всі інформаційні ресурси взаємопов'язані та контролюються централізованими контролерами.

Якщо ви отримаєте доступ до одного інформаційного ресурсу в хмарі, всі інші знаходяться під загрозою. Замість того, щоб накопичувати різні системи безпеки у хмарній службі, ефективніше впроваджувати підроблені інформаційні ресурси.

Вирішити цю проблему пропонується за допомогою технології мережевої "приманки". Бажано використовувати мережу "приманок" у хмарній службі як послугу (HaaS). Це дозволяє зменшити початкові та експлуатаційні витрати на підтримку Інфраструктури, підвищити ефективність розгортання системи та забезпечити можливість віддаленого управління.

Список літератури

[1]. Vitalii Susukailo, Ivan Opirskyy, Sviatoslav Vasylyshyn, Analysis of the use of software baits as a means of ensuring information security, *2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*. – p. 242-245.

[2]. John Wiley. Carbon Black Special Edition, Inc. 111 River St. Hoboken, NJ 070305774. "*Threat Hunting For Dummies*®", 2017. – 53 p.

[3]. Huijun Wu, Dijiang Huang. *Mobile Cloud Computing: Foundations and Service Models (1st. ed.)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2017. – 336 p.

[4]. Jeff Petters. *Varonis. Endpoint Detection and Response (EDR): Everything You Need to Know*, 2017 [Електронний ресурс] – [Режим доступу] https:// www. varonis.com/blog/endpoint-security/.

[5]. Oleksandr Milov, Alexander Voitko, Iryna Husarova, Oleg Domaskin, Yevheniia Ivanchenko, Ihor Ivanchenko, Olha Korol, Hryhorii Kots, Ivan Opirskyy, Oleksii Fraze-Frazenko. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems, *Eastern-european journal of enterprise technologies. Information and controlling system*. – Vol 2, No 9(98), 2019. – pp. 56-66.

[6]. Khan, Z.A.; Abbasi, U. "*Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things*". Electronics 2020, 9, 415. – 30 p.

[7]. Akiyama M., Yagi T., Hariu T., *Honey Circulator: distributing credential honeytoken for introspection of web-based attack cycle*. Int. J. Inf. Secur. 17, 2018. – pp. 135–151.

[8]. Rich Mogull, James Arlen, Francoise Gilbert, Adrian Lane, David Mortman, Gunnar Peterson, Mike Rothman *The Security Guidance for Critical Areas of Focus in Cloud Computing* v4.0, 2017 Cloud Security Alliance. – 152 p.

УДК 654.071

Opirskyy I.R., Vasylyshyn S.I., Susukailo V.A.. Investigating cybercrime with honeypots in the cloud

Abstract. *Cloud technologies are increasingly used. While a cloud environment can give organizations the freedom to experiment and scale resources, it also increases the surface area of attack. This article explores the possibilities of baits in cloudy environments. Analyzes the problem of investigating cybercrimes in the clouds. Identifies and studies relevant technologies used by cybersecurity professionals in the investigation of cybercrime. Determines the benefits of using baits in cloud infrastructure. For cloud environments, the number one threat is data breaches. Violations can cause great reputational and financial damage. They can potentially lead to the loss of intellectual property and significant legal obligations. Inadequate access control, in a cloud environment, is a threat that can compromise the cloud system. To avoid this threat, cloud clients must protect credentials, provide automatic rotation of cryptographic keys, passwords, and certificates, ensure scalability, require cloud service administrators to use multi-factor authentication, and define password policies for the management plane and each service deployed in the cloud. The trap provides significant benefits to security*

professionals. First of all, it is a collection of necessary information, often containing valuable information. Deployment and operation of baits is not particularly difficult, and trap tools usually do not require system resources. Particular attention should be paid to the insttion and operation of traps. As a rule, the whole range of measures is reduced to "establishment and expectation". The most common case is with a dedicated server under the supervision of specialists. Today, there are many fake programs that give the impression of real, but not true, their main task - to record the entire exchange. The advantage of the trap is that a copy of the software can be made on an obsolete server that cannot cope with the typical computational tasks of e-business. It is determined that it is recommended to use the network of "baits" in the cloud service as a service (HaaS). This reduces the initial and operating costs of maintaining the Infrastructure, increases the efficiency of system deployment and provides remote management.
Key words: *honeypot, cloud environment, cloud infrastructure, cybercrime, Amazon web services, cloud platform Azure, IaaS, PaaS, SaaS.*

Опирский И.Р., Василишин С.І., Сусукайло В.А. Расследование киберпреступлений с помощью приманок в облачной среде

Аннотация. *Облачные технологии все чаще используются. Хотя облачную среду может дать организациям свободу экспериментировать и масштабировать ресурсы, оно также увеличивает поверхность атаки. Эта статья исследует возможности приманок в облачных средах. Анализирует проблему расследования киберпреступлений в облаках. Определяет и изучает соответствующие технологии, используемые специалистами по кибербезопасности при расследовании киберпреступлений. Определяет преимущества использования приманок в облачной инфраструктуре. Для облачных сред угрозой номер один является нарушение данных. Нарушения могут нанести большой репутационный и финансовый ущерб. Они могут потенциально привести к потере интеллектуальной собственности и значительных юридических обязательств. Неадекватное управление доступом, в облачной среде, угроза, что может привести к компрометации облачной системы. Чтобы избежать этой угрозы, клиенты облака должны защищать учетные данные, обеспечивать автоматическое вращение криптографических ключей, паролей и сертификатов, обеспечивать масштабируемость, требовать от администраторов облачных служб использование многофакторной аутентификации, определять политику паролей для плоскости управления и каждой службы, развернутой в облаке. Определено, что рекомендуется использовать сеть "приманок" в облачной службе как услугу (HaaS). Это позволяет уменьшить начальные и эксплуатационные затраты на поддержание инфраструктуры, повысить эффективность развертывания системы и обеспечить возможность удаленного управления.*
Ключевые слова: *приманка, облачную среду, облачная инфраструктура, киберпреступность, веб-службы Amazon, облачная платформа Azure, IaaS, PaaS, SaaS.*

Опірський Іван Романович, доктор технічних наук, професор, професор кафедри захисту інформації Національного університету "Львівська політехніка".
Опирский Иван Романович, доктор технических наук, профессор, профессор кафедры защиты информации Национального университета "Львовская политехника".
Opirskyy Ivan Romanovych, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security of the National University "Lviv Polytechnic".

Василишин Святослав Ігорович, аспірант, асистент кафедри Захисту інформації в національному університеті "Львівська політехніка".
Василишин Святослав Игоревич, аспирант, ассистент кафедры Защиты Информации в национальном университете "Львовская политехника".
Sviatoslav Vasylyshyn, postgraduate student, Assistant at the Lviv Polytechnic National University (Information security).
Сусукайло Віталій Андрійович, аспірант кафедри Захисту інформації в національному університеті "Львівська політехніка".
Сусукайло Виталий Андреевич, аспирант кафедры Защиты Информации в национальном университете "Львовская политехника".
Vitalii Susukailo, postgraduate student at the Lviv Polytechnic National University (Information security).

Отримано *15 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*

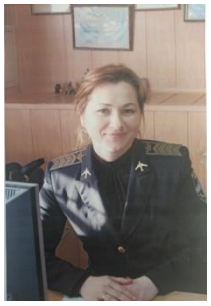
БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ / E-GOVERNANCE SECURITY

DOI: 10.18372/2225-5036.26.15575

СУЧАСНІ КОМПЛЕКСИ ПОСТ-КВАНТОВОЇ БЕЗПЕКИ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Анна Корченко, Євгенія Іванченко, Наталія Кошкіна, Олександр Кузнецов, Олена Качко, Олександр Потій, Віктор Онопрієнко, Всеволод Бобух

КОРЧЕНКО Анна Олександрівна, д.т.н., доцент.
Рік і місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, системи виявлення вторгнень, експертне оцінювання в сфері захисту інформації.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: annakor@ukr.net.
ORCID: 0000-0003-0016-1966.



ІВАНЧЕНКО Євгенія Вікторівна, к.т.н., професор.
Рік і місце народження: 1976 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2000 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, системи виявлення вторгнень, безпека хмарних технологій.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: evivancenko@gmail.com.
ORCID: 0000-0003-3017-5752.

КОШКІНА Наталія Василівна, д.т.н., с.н.с.
Рік та місце народження: 1977 рік, с. Велика Чернеччина, Сумська обл., Україна.
Освіта: Сумський державний педагогічний інститут ім. А.С. Макаренка, 1999.
Посада: старший науковий співробітник Інституту кібернетики ім. В.М. Глушкова НАН України з 2008 р.
Наукові інтереси: інформаційна та кібербезпека, стеганографія, стеганоаналіз.
Публікації: більше 50 наукових публікацій, серед яких монографії, наукові статті та тези.
E-mail: nata.koshkina@gmail.com.
ORCID: 0000-0001-5180-2255.

КУЗНЕЦОВ Олександр Олександрович, д. т. н., професор
Рік та місце народження: 1974 рік, м. Харків, Україна.
Освіта: Харківський військовий університет, 1996 рік.
Посада: професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук Харківського національного університету імені В.Н. Каразіна з 2008 р.
Наукові інтереси: інформаційна та кібербезпека, теорія інформації та кодування, криптографія та стеганографія.
Публікації: більше 300 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: kuznetsov@karazin.ua.
ORCID: 0000-0003-2331-6326.

Качко Олена Григорівна, к.т.н., професор.
Рік та місце народження: 1945 рік, м. Ізюм, Харківської області, Україна.
Освіта: Харківський національний університет радіоелектроніки (Харківський інститут радіоелектроніки), 1967 рік.
Посада: професор кафедри програмної інженерії, з 1999 р., заступник головного конструктору АТ «ІІТ» з 2011р.
Наукові інтереси: інформаційна та кібербезпека, теорія та практика розробки паралельних програм.
Публікації: більше 70 наукових публікацій, серед яких, навчальні посібники, монографії, наукові статті та тези.
E-mail: elena.kachko@nure.ua.
ORCID: 0000-0001-9249-0497.

ПОТІЙ Олександр Володимирович, д.т.н., професор, полковник.
Рік та місце народження: 1971 рік, м. Кривий Ріг, Україна.
Освіта: Харківське вище воєнне командно-інженерне училище ракетних військ стратегічного призначення, 1993 рік; Харківський військовий університет, 1996; Харківський університет Повітряних Сил, 2008.
Посада: Заступник Голови Державної служби спеціального зв'язку та захисту інформації України з 2020 р.
Наукові інтереси: інформаційна та кібербезпека, менеджмент інформаційної безпеки, криптографія.
Публікації: більше 100 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові та методичні статті та тези, національні стандарти, нормативні документи та навчальні курси, патенти.
E-mail: potav1971@gmail.com.
ORCID: 0000-0002-2366-0541.

ОНОПРІЄНКО Віктор Васильович, к.т.н.
Рік та місце народження: 1958 рік, с. Горбані, Переяслав-Хмельницький район, Київська обл., Україна.
Освіта: Київське вище інженерне радіотехнічне училище ППО, 1981 р.
Посада: Генеральний директор з 2015 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 8 наукових публікацій, серед яких, наукові статті.
E-mail: v25258@gmail.com.
ORCID: 0000 0002 1174 8968.

БОБУХ Всеволод Анатолійович, к.т.н.
Рік та місце народження: 1981 рік, м. Харків, Харківська обл., Україна.
Освіта: Харківський національний університет радіоелектроніки, 2002 рік.
Посада: начальник відділу апаратних засобів захисту інформації Приватного акціонерного товариства "Інститут інформаційних технологій".
Наукові інтереси: апаратні та апаратно-програмні засоби захисту інформації.
Публікації: більше 30 наукових публікацій, серед яких монографії, наукові статті, тези та патенти.
E-mail: bobukhv@iit.kharkov.ua.
ORCID: 0000-0002-1175-5092.

Анотація. *На теперішній час в умовах широкого впровадження в економіку, оборонну і безпекову сфери цифрових технологій в усіх провідних державах світу гостро стоїть проблема забезпечення безпеки їх кіберпростору, особливо в умовах нових загроз, що породжуються використанням квантових комп'ютерів. Тому створення в Україні відповідної системи безпеки кіберпросторового довкілля національної критичної інформаційної інфраструктури, зокрема комплексів та засобів виявлення вторгнень, криптографічного та стеганографічного захисту інформації, є сучасною та актуальною проблематикою, що безпосередньо стосується пост-квантової інформаційної та кібербезпеки нашої держави, а також має важливе загальнодержавне та оборонне значення і суттєво впливає на забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн. Виходячи з актуальності проблеми забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн, метою є удосконалення систем спеціального призначення за рахунок побудови комплексів криптографічного захисту інформації пост-квантової безпеки Державних електронних інформаційних ресурсів. Реалізовано проекти з розробки та впровадження програмно-технічних комплексів та апаратних засобів КЗІ для надавачів електронних довірчих послуг*

Збройних сил України, Міністерства внутрішніх справ, Державної прикордонної служби, Державної податкової служби України, Національного банку України, Приватбанку, Укрсіббанку, Альфа банку тощо, включно по два технологічні центри сертифікації ключів для Центрального засвідчувального органу України та засвідчувального центру Національного банку України. Таким чином, розроблені програмно-технічні комплекси та апаратні засоби КЗІ створили безпечне пост-квантове довкілля для державних електронних інформаційних ресурсів.

***Ключові слова**: мереж передачі даних спеціального призначення, криптографічні засоби, комплекси спеціального призначення, засоби захисту інформації, кіберпростір, пост-квантове довкілля, державні електронні інформаційні ресурси.*

Вступ

На даний час в умовах широкого впровадження в економіку, оборонну і безпекову сфери цифрових технологій в усіх провідних державах світу гостро стоїть проблема забезпечення безпеки їх кіберпростору, особливо в умовах нових загроз, що породжуються використанням квантових комп'ютерів

Для України ця проблема ще більш актуальна, адже з 2014 року проти нашої держави йде широкомасштабна гібридна та інформаційна агресія, одним з ефективних елементів якої є високотехнологічні впливи на державну інформаційну та критичну інфраструктуру.

Тому створення в Україні відповідної системи безпеки кіберпросторового довкілля, національної критичної інформаційної інфраструктури [2], зокрема комплексів та засобів виявлення вторгнень [3, 4], криптографічного [1] та стеганографічного [5] захисту інформації, є сучасною та актуальною проблематикою, що безпосередньо стосується пост-квантової інформаційної та кібербезпеки нашої держави, а також має важливе загальнодержавне та оборонне значення і суттєво впливає на забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн.

На теперішній час нашій державі створено необхідні засади для розгортання та побудови високотехнологічних пост-квантових безпечних мереж передачі даних спеціального призначення виключно на вітчизняному обладнанні криптографічного захисту інформації (КЗІ).

У [6] авторами роблено основні елементи загальнодержавної системи КЗІ, що стали основою стандартизації систем, комплексів та засобів КЗІ пост-квантової безпеки.

Для України актуальним є створення реальної системи пост-квантової безпеки. Це пов'язане з необхідністю розробки комплексів КЗІ для забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими і серверними частинами прикладних систем (TCP-з'єднань) або у розподілених системах на основі IP-мереж передачі даних.

Зазначені функції комплекси повинні виконувати шляхом застосування механізмів КЗІ, яка передається між клієнтом та сервером, зовнішніми каналами зв'язку або у вигляді мережевого IP-потоку між розподіленими локальними обчислювальними мережами (далі – ЛОМ) або між клієнтами та ЛОМ через зовнішні канали зв'язку.

Мета роботи

Виходячи з актуальності проблеми забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн, метою роботи є удосконалення систем спеціального призначення за рахунок побудови комплексів КЗІ пост-квантової безпеки державних електронних інформаційних ресурсів.

Постановка задачі

Для досягнення поставленої мети необхідно розробити технічні характеристики та побудувати криптографічні засоби захисту інформації для використання у вітчизняних комплексах спеціального призначення та обґрунтувати доцільність використання окремих рішень та виконаних впроваджень вітчизняних засобів захисту інформації при побудові мереж та комплексів спеціального призначення на рівні держави. Стосовно захисту електронних інформаційних ресурсів, розглянемо основні результати з розробки та дослідження зазначених засобів захисту інформації та їх практичне застосування в пост-квантовому довкіллі, основою побудови яких слугували наукові результати, отримані в [6].

Комплекс користувача ЦСК "ІІТ РИСТУВАЧ ЦСК-1"

Комплекс у складі системи електронного документообігу чи іншої прикладної системи (далі - системи) призначений для: автентифікації користувачів системи при підключенні до сервера та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером; забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Зазначені функції комплекс виконує шляхом застосування механізмів КЗІ, яка обробляється у системі. Автентифікація користувачів системи на сервері здійснюється під час підключення користувачів до сервера (встановлення з'єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером системи під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, реалізуються шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача системи так і на стороні сервера. Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритми шифрування за

ДСТУ ГОСТ 28147: 2009 та TDEA і AES за ISO/IEC 18033-3:2010; алгоритми ЕЦП за ДСТУ 4145-2002, RSA за PKCS#1 (RFC 3447) та ECDSA за ДСТУ ISO/IEC 14888-3:2014; алгоритми гешування за ГОСТ 34.311-95 та SHA (SHA-1 і SHA-224/256/ 384/512) за ДСТУ ISO/IEC 10118-3:2005; протоколи розподілу ключів за ДСТУ ISO/IEC 15946-3 (пп. 8.2) та RSA за PKCS#1 (RFC 3447).

Протоколи розподілу ключових даних реалізуються згідно ДСТУ ISO/IEC 15946-3 і вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р., та за алгоритмом направленого шифрування RSA згідно PKCS#1 (RFC 3447). Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України.

Протокол встановлення захищеного сеансу передачі даних користувачем та сервером реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3. Протокол взаємної автентифікації включає: формування користувачем та передачу даних автентифікації (запиту) на сервер; обробку запиту від користувача сервером; прийом та обробку відповіді користувача від сервера.

За результатом роботи протоколу на сервері та користувачеві встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES.

В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з'єднанні використовуються коди автентифікації повідомлень (імітовставки), які обчислюються за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES.

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та сервера системи.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера системи відносяться особисті ключі та сертифікати відповідно користувачів та сервера. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"), Aladdin eToken/JaCarta, Автор SecureToken, Технотрейд uaToken, SafeNet iKey, Giesecke&Devrient StarSign, Gemalto IDPrime, ДБОСофт iToken та Ефіт Key; смарт-карти "Карта-1" ("ІІТ Смарт-карта Карта-1"), Техноконсалтинг TEllipse, Aladdin eToken /JaCarta, Автор CryptoCard, Giesecke &Devrient StarSign та ДБОСофт Інтегра; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера системи, надання послуг фіксування часу, а також надання (за необхідності) користувачам системи засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів користувачів та сервера системи; надання послуг фіксування часу; надання користувачам системи (за необхідності) засобів генерації особистих та відкритих ключів.

Для взаємодії з центром сертифікації ключів (використання його інтерактивних служб) користувачі та сервери системи повинні мати можливість мережевого підключення до ЦСК. Усі механізми взаємодії з ЦСК виконують бібліотеки користувача ЦСК.

Зміна статусу сертифікатів (блокування, поновлення або скасування) та знищення особистих ключів користувачів та сервера системи здійснюється у відповідності до порядку, який визначений ЦСК (згідно регламенту ЦСК).В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

До складу комплексу входять: програмні засоби (бібліотеки) КЗІ (користувача ЦСК) "ІІТ Користувач ЦСК-1"; апаратні засоби КЗІ. До складу апаратних засобів комплексу можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301"). Структурна схема комплексу захисту наведена на рис. 1.

Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси. Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережеві криптомодулі тощо.

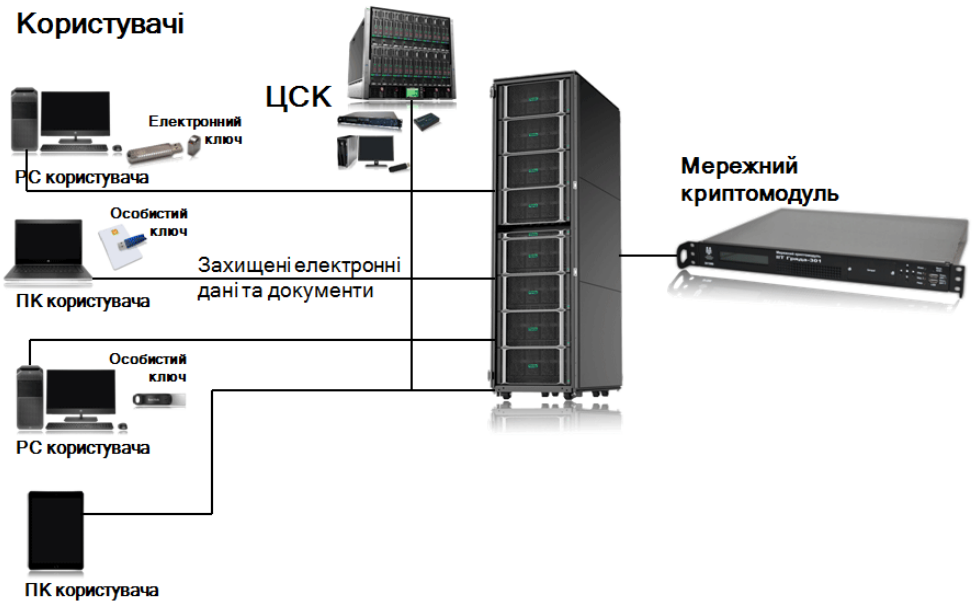


Рис. 1. Структурна схема комплексу захисту

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС), що включає зашифрування та розшифрування даних, формування та перевірку ЕЦП від даних, захист сеансів передачі даних (захист з'єднань; інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК); отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Бібліотеки користувача ЦСК інтегруються у зазначену систему (та інші прикладні системи) через визначені інтерфейси (Microsoft CSP, PKCS#11, GSS-API, JCA) і власні та реалізовані для ОС Microsoft Windows, Linux (SuSe/Red Hat/Ubuntu /Cent OS та ін.), UNIX (IBM AIX/Sun Solaris/Free BSD та ін.), Apple macOS/iOS, Google Android у вигляді бібліотек підключення (DLL/COM, SO, DyLib – 32/64-біта) або у вигляді архівів java-класів для JRE чи java-скриптів тощо. Для всіх бібліотек користувача ЦСК під всі ОС та платформи, що підтримуються, існують приклади використання. Бібліотеки користувача ЦСК інтегровані у різні прикладні системи, серед яких: більше 200 корпоративних та внутрішньовідомчих систем, а також електронних реєстрів тощо; системи електронної пошти (поштові клієнти та сервери): Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС-Он-Лайн Foss Mail та ін.; офісні пакети: Microsoft Office, Adobe Acrobat та ін.; системи електронного документообігу: Інфо+ АСКОД, ТрансЛінкКонсалтинг Док-Проф, Софтлайн Мегаполіс та ін.; системи подання звітності у електронному вигляді до Державної податкової служби України, Пенсійного фонду України, Держфінмоніторингу, МВС України та ін.; автоматизовані та інтегровані банківські системи: SAP for Banking, Oracle FlexCube та ін.; власні засоби та комплекси КЗІ.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів користувача системи. Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера системи. На сервері системи встановлюються та використовуються наступні складові частини комплексу: програмний комплекс захисту сервера, який включає бібліотеки користувача ЦСК (для відповідної серверної ОС); апаратний засіб КЗІ - мережевий криптомодуль.

На засобах користувачів системи (робочих станціях чи портативних комп'ютерах - РС та ПК) встановлюються та використовуються наступні складові частини комплексу: програмний комплекс захисту користувача, який включає бібліотеки користувача ЦСК (для відповідної ОС); апаратний засіб КЗІ - електронний ключ. Електронний ключ "Кристал-1" призначений для: автентифікації користувача системи перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача.

Мережевий криптомодуль "Гряда-301" призначений для: автентифікації сервера системи перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до сервера системи безпосередньо або через комутатори локальної обчислювальної мережі. Апаратна реалізація мережевого криптомодуля забезпечує

захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку сервера системи.

Програмно-технічний комплекс центру сертифікації КЛЮЧІВ (ЦСК) "ІІТ ЦСК-1"

Призначення комплексу: реалізація ЦСК регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів ЦСК (далі – користувачів), надання послуг фіксування часу, надання користувачам засобів ЕЦП та шифрування, а також засобів генерації особистих і відкритих ключів. Технічні засоби комплексу об'єднані у ЛОМ з використанням внутрішньої комунікаційної мережі з наявністю підключення до зовнішніх комунікаційних мереж.

Окремі технічні засоби комплексу ізольовані від мереж передачі даних. Порядок експлуатації комплексу у складі ЦСК відповідає вимогам правил посиленої сертифікації. Структурна схема комплексу наведена нижче (рис. 2).

Комплекс забезпечує реалізацію регламентних процедур та механізмів роботи ЦСК, пов'язаних з: обслуговуванням сертифікатів відкритих ключів (далі – сертифікатів) користувачів, що включає: реєстрацію користувачів, сертифікацію відкритих ключів користувачів, розповсюдження сертифікатів, управління статусом сертифікатів, розповсюдження інформації про статус сертифікатів; надання послуг фіксування часу; надання користувачам засобів ЕЦП та шифрування даних, а також засобів генерації та управління ключами.

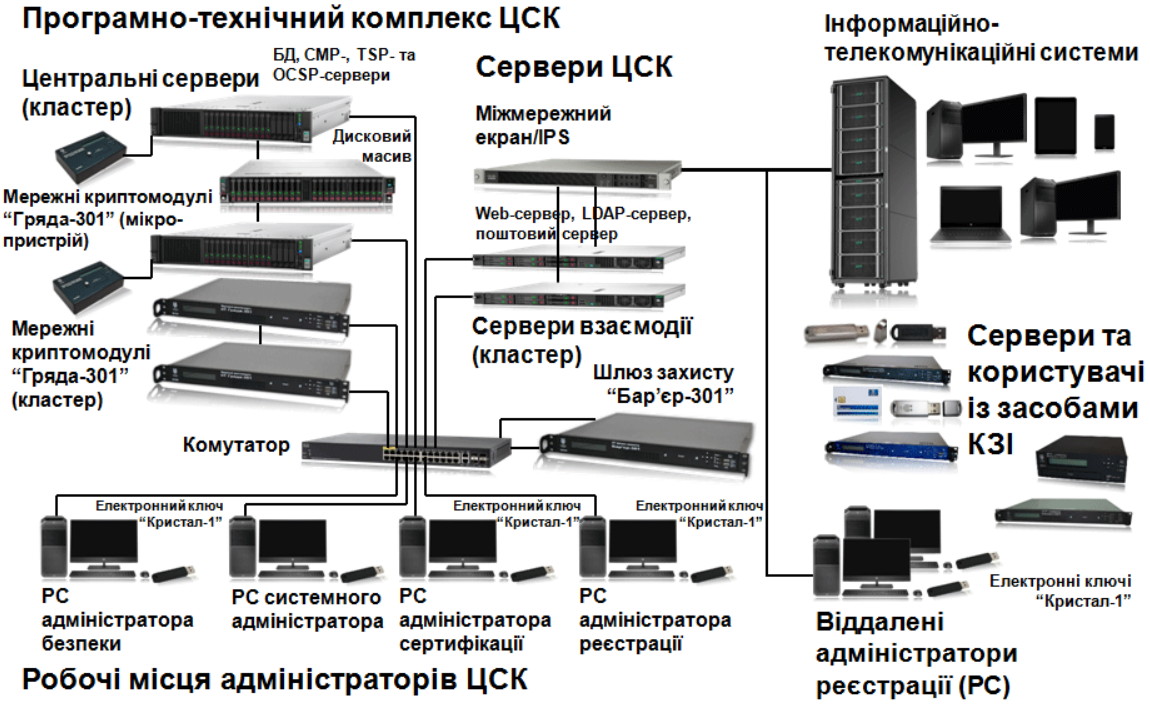


Рис. 2. Структурна схема комплексу

Комплекс забезпечує виконання наступних функцій, пов'язаних з обслуговуванням ЦСК сертифікатів користувачів: реєстрацію користувачів; сертифікацію відкритих ключів користувачів; розповсюдження сертифікатів відкритих ключів користувачів; управління статусом сертифікатів відкритих ключів користувачів та розповсюдження інформації про статус сертифікатів. Комплекс забезпечує виконання наступних функцій, пов'язаних з наданням ЦСК послуг фіксування часу: приймання та реєстрацію запитів користувачів на формування позначок часу; формування позначок часу; передачу сформованих позначок часу користувачам; внесення сформованих позначок часу у базу даних; зберігання сформованих позначок у базі даних; архівування бази даних позначок часу. До складу комплексу входять засоби користувачів у складі: засобів генерації особистих і відкритих ключів користувачів, які призначені для генерації особистого та відкритого ключів користувача, формування та передачу запиту на формування сертифіката користувача до ЦСК, отримання, перевірку, зберігання та використання сформованого сертифікату, формування та передачу запитів на блокування, скасування та поновлення сертифіката користувача до ЦСК; засобів ЕЦП та шифрування даних користувачів.

До складу комплексу входять такі технічні засоби: робочі станції (РС) обслуговуючого персоналу (адміністратора безпеки, системного адміністратора та адміністратора реєстрації); центральні сервери (сервери ЦСК); внутрішнє комунікаційне обладнання локальної обчислювальної мережі (ЛОМ); сервери взаємодії; міжмережевий екран (МЕ) та система виявлення втручань (IDS); комунікаційне обладнання для підключення до зовнішніх комунікаційних мереж (ЗКМ); РС генерації ключів користувачів (ізольована); РС віддалених адміністраторів реєстрації (відокремлені).

Окремо (до складу програмно-технічного комплексу відокремленого пункту реєстрації) входить РС віддаленого адміністратора. РС адміністратора безпеки, адміністратора сертифікації, системного адміністратора, адміністратора реєстрації, центральні сервери та сервери взаємодії мають взаємодіяти через внутрішню комунікаційну мережу на основі кабельної мережі та комутаторів і утворювати ЛОМ. Центральні сервери, сервери взаємодії, їх ДБЖ, мережевий комутатор, комутатор терміналів, МЕ, а також криптомодулі і мережні криптомодулі мають бути розміщені у екранованій шафі чи у звичайні шафі у екранованому приміщенні.

У випадку, якщо функції центральних серверів, що пов'язані з формуванням сертифікатів та списків відкликаних сертифікатів (під час яких використовується особистий ключ ЦСК) виконує РС адміністратора сертифікації, вона має бути реалізована на основі ПЕОМ у захищеному виконанні або розміщена у екранованій кабіні чи екранованому приміщенні. Сервери можуть бути з'єднані у окрему ЛОМ з використанням власного комутатора та підключатися до комутатора РС через електричний кабель або волоконно-оптичну лінію зв'язку (ВОЛЗ). Можливе також об'єднання комутаторів серверів та РС у один спільний комутатор ЛОМ. У цьому випадку РС обслуговуючого персоналу підключають до комутатора окремими електричними кабелями чи ВОЛЗ.

Сервери взаємодії мають підключатися до зовнішньої комунікаційної мережі через зовнішній МЕ (із вбудованою IPS). Для підключення серверів взаємодії до комутатора та до МЕ мають використовуватися різні мережні адаптери.

МЕ з IPS мають підключатися до зовнішньої комунікаційної мережі через комунікаційне обладнання оператора послуг передачі даних через електричний кабель або через ВОЛЗ. У випадку використання для такого підключення ВОЛЗ, мають використовуватися або оптичні мережні порти МЕ або конвертори довкілля.

Для забезпечення централізованого моніторингу роботи складових частин комплексу до його складу може входити система моніторингу. Серверна частина системи моніторингу може встановлюватися на РС системного адміністратора або на окремий сервер моніторингу, а на всі сервери та РС комплексу мають бути встановлені агенти системи моніторингу. Взаємодія сервера з агентами моніторингу здійснюється за внутрішнім протоколом, а з іншими вузлами - за стандартними протоколами моніторингу (syslog, SNMP тощо). Комплекс взаємодіє з ПТК центрів та ІТС інших зовнішніх користувачів через сервери взаємодії. Функціональною основою комплексу є спеціалізовані апаратні та програмні засоби КЗІ і включає: програмний комплекс ЦСК "ІІТ ЦСК-1"; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301"); програмний комплекс віддаленого адміністратора реєстрації ЦСК "ІІТ ЦСК-1. Віддалений адміністратор реєстрації"; програмний комплекс користувача ЦСК "ІІТ Користувач ЦСК-1"; електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"). Мережевий криптомодуль "Гряда-301" (мікро-пристрій) призначений для апаратної реалізації формування ЕЦП і у складі центральних серверів чи РС адміністратора сертифікації і забезпечує використання та захист особистого ключа ЦСК. Особистий ключ ЦСК генерується, зберігається та використовується тільки у середині пристрою. Мережевий криптомодуль "Гряда-301" призначений для апаратної реалізації криптографічних перетворень у складі центральних серверів ЦСК (CMP, TSP та OCSP).

У складі програмного забезпечення користувачів ЦСК може використовуватися апаратний електронний ключ "Кристал-1". Електронний ключ призначений для апаратної реалізації криптографічних перетворень. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку апаратно-програмного довкілля.

Комплекс забезпечує функціональні характеристики, що наведені у табл. 1 та надавати доступ до ЦСК користувачам цілодобово 7 днів на тиждень.

Центральні сервери та сервери взаємодії можуть функціонувати автоматизовано. Існує можливість роботи серверів у різних режимах - основний чи резервний з повним чи частковим дублюванням функцій. Функціональні характеристики та режими експлуатації комплексу не залежать від типів та характеристик технічних засобів (РС, серверів та комунікаційного обладнання). У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритми шифрування за ДСТУ ГОСТ 28147:2009 та TDEA і AES за ISO/IEC 18033-3:2010; алгоритми ЕЦП за ДСТУ 4145-2002, RSA за PKCS#1 (RFC 3447) та ECDSA за ДСТУ ISO/IEC 14888-3:2014; алгоритми гешування за ГОСТ 34.311-95 та SHA (SHA-1 і SHA-224/256/384/512) за ДСТУ ISO/IEC 10118-3:2005; протоколи розподілу ключів за ДСТУ ISO/IEC 15946-3 (пп. 8.2) та RSA за PKCS#1 (RFC 3447).

Протоколи розподілу ключових даних реалізуються згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) і вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р., та за алгоритмом направленого шифрування RSA згідно PKCS#1 (RFC 3447).

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України.У ключовій системі комплексу виділені дві підгрупи ключових даних: службові ключові дані; ключові дані користувачів.

До складу службових відносяться: особистий ключ та сертифікат ЦСК; особисті ключі та сертифікати серверів ЦСК (CMP, TSP та OCSP); особисті ключі та сертифікати адміністраторів реєстрації та віддалених адміністраторів реєстрації. Особистий ключ ЦСК зберігається та застосовується тільки у криптомодулі, що входить до складу сервера ЦСК або РС адміністратора сертифікації. Особистий ключ ЦСК використовується для формування ЕЦП сертифікатів та списків відкликаних сертифікатів.

Сертифікат ЦСК використовується для перевірки ЕЦП, що накладається за допомогою особистого ключа ЦСК. Особисті ключі серверів ЦСК (OCSP та TSP) використовується для формування ЕЦП від позначок часу та інформації про статус сертифікатів.

Сертифікати серверів ЦСК використовується для перевірки ЕЦП, що накладається за допомогою відповідних особистих ключів серверів ЦСК.

Особисті ключі адміністраторів реєстрації та віддалених адміністраторів реєстрації призначені для формування ЕЦП запитів на формування сертифікатів, а також запитів на блокування, поновлення та скасування, а сертифікати – для перевірки ЕЦП від вказаних типів даних.

Ключі віддалених адміністраторів реєстрації призначені також для шифрування даних, що передаються між РС віддаленого адміністратора реєстрації та ЦСК (CMP-сервером ЦСК).

Таблиця 1

Функціональні характеристики комплексу

Показник	Значення
Кількість користувачів, яких обслуговує комплекс	не менше 1 000 000
Кількість користувачів, які можуть зареєструватися	не менше 5 000 за добу
Кількість користувачів, які одночасно мають доступ до сервера взаємодії (LDAP-каталогу та web-сторінки)	не менше 5 000
Час обробки запитів користувачів на формування, блокування, поновлення та скасування сертифікатів сервером ЦСК	не більше 1 с(не менше 100 запитів/с)
Час обробки запитів зовнішніх користувачів на визначення статусу сертифіката	не більше 1 с(не менше 500 запитів/с)
Час обробки запитів зовнішніх користувачів на формування позначки часу	не більше 1 с (не менше 500 запитів/с)

До ключових даних користувачів відносяться особисті ключі та сертифікати користувачів. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"), Aladdin eToken/JaCarta, Автор SecureToken, SafeNet iKey, Giesecke&Devrient StarSign, Gemalto IDPrime, ДБОСофт iToken та Ефіт Key; смарт-карти "Карта-1" ("ІІТ Смарт-карта Карта-1"), Техноконсалтинг TEllipse, Aladdin eToken/Ja Carta, Автор CryptoCard, Giesecke &Devrient StarSign та ДБОСофт Інтегра; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Комплекс захисту електронної пошти "ІІТ ЗАХИЩЕНА ЕЛЕКТРОННА ПОШТА"

Призначення комплексу: захист електронних поштових повідомлень при передачі та зберіганні. Захист забезпечується шляхом підпису повідомлень з використанням електронного цифрового підпису, а також шифруванням повідомлень користувача у поштовому клієнті (та сервері) при передачі та зберіганні.

Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК).

Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рис. 3.

До складу комплексу входять: програмні засоби КЗІ (програмні засоби захисту електронної пошти "ІІТ Захищена електронна пошта" для різних поштових клієнтів; бібліотеки користувача ЦСК зі складу програмного комплексу користувача ЦСК "ІІТ Користувач ЦСК-1"); апаратні засоби КЗІ.

До складу апаратних засобів комплексу можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Засоби захисту електронної пошти реалізують наступні функції: зашифрування електронних повідомлень; розшифрування електронних повідомлень; зашифрування та підпис електронних повідомлень; розшифрування та перевірку електронних повідомлень; відображення інформації про відправника захищеного електронного повідомлення та ін.

Програмні засоби захисту електронної пошти реалізують логіку роботи комплексу та інтегровані безпосередньо у поштові клієнти (та поштові сервери), через визначені механізми та інтерфейси.

Засоби захисту електронної пошти інтегровано у поштові клієнти Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС-Он-Лайн FossMail та ін., а також у спеціалізовані поштові сервери для окремих поштових клієнтів. Програмні засоби захисту електронної пошти можуть функціонувати у ОС Microsoft Windows 2000/ XP/2003 Server /7/ 2008 Server, Linux (SUSE/ Red Hat /Slackware та ін.) та UNIX (AIX/Solaris/BSD та ін.). Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо. Бібліотеки користувача центру

сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ. Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів поштового клієнта.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі поштового сервера системи.

Електронний ключ "Кристал-1" призначений для: автентифікації користувача (поштового клієнта) перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача.

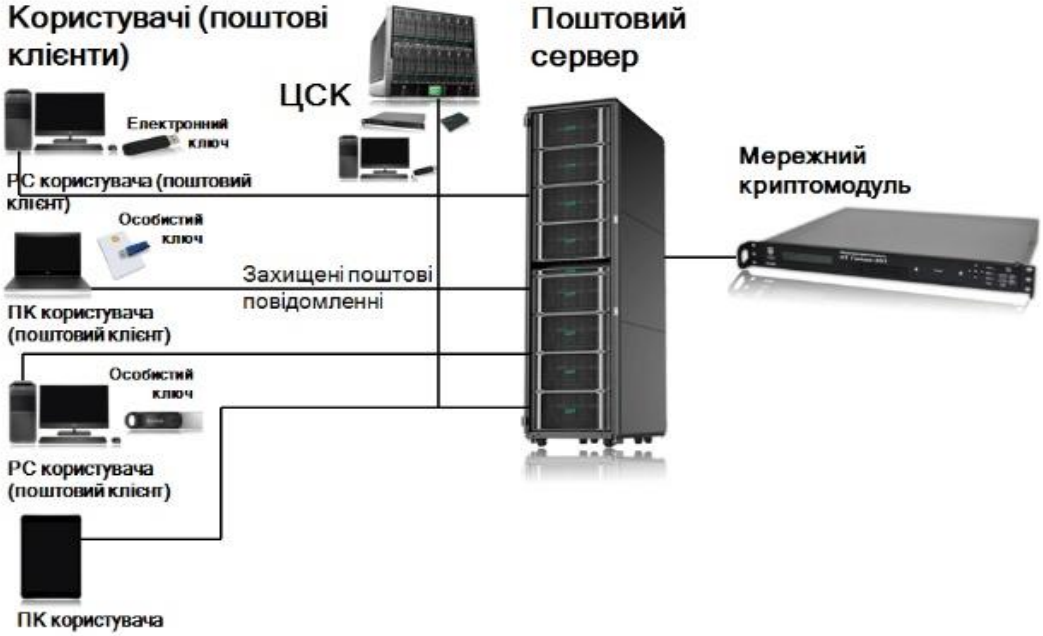


Рис. 3. Структурна схема комплексу

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача.

Мережевий криптомодуль "Гряда-301" призначений для: автентифікації поштового сервера перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/1000 для підключення до поштового сервера безпосередньо або через комутатори локальної обчислювальної мережі.

У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку. Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК).

У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані клієнтів (користувачів) та серверів.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних клієнтів (користувачів) та серверів відносяться особисті ключі та сертифікати відповідно користувачів та серверів.

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS# 11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог

до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12. Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів клієнтів (користувачів) та серверів, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів (користувачів) та серверів; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Комплекс захисту мережних з'єднань (TCP/IP) "ІІТ ЗАХИСТ З'ЄДНАНЬ-2"

Призначення комплексу: забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими та серверними частинами прикладних програмних систем (TCP-з'єднань).

Комплекс забезпечує: автентифікацію клієнтської частини прикладних програмних систем при підключенні до серверної частини; встановлення захищеного TCP-з'єднання між клієнтом та сервером; шифрування даних TCP-з'єднання, які передаються між клієнтом та сервером. Зазначені функції комплекс виконує шляхом застосування механізмів КЗІ, яка передається між клієнтом та сервером.

Комплекс підтримує взаємодію клієнтських та серверних частин (програмного забезпечення) прикладних програмних систем за протоколом TCP/IP. Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рис. 4. До складу комплексу входять: шлюз захисту (програмний комплекс "ІІТ Захист з'єднань-2. Шлюз захисту" або апаратний засіб - шлюз захисту "ІІТ ШЗ Бар'єр-301/ 301 (міні-пристрій)/301 (мікро-пристрій)"); програмний комплекс управління (віддаленого) шлюзами захисту "ІІТ Захист з'єднань-2. Віддалене управління шлюзами захисту"; програмний комплекс агента моніторингу шлюзів захисту "ІІТ Захист з'єднань-2. Агент моніторингу шлюзів захисту"; програмний комплекс моніторингу шлюзів захисту "ІІТ Захист з'єднань-2. Монітор шлюзів захисту"; програмний комплекс клієнта захисту "ІІТ Захист з'єднань-2. Клієнт"; proxy-клієнт захисту (програмний комплекс "ІІТ Захист з'єднань-2. Proxy захисту", далі – proxy захисту); програмний комплекс агента моніторингу proxy захисту "ІІТ Захист з'єднань-2. Агент моніторингу proxy захисту"; програмний комплекс моніторингу proxy захисту "ІІТ Захист з'єднань-2. Монітор proxy захисту"; програмний комплекс VPN-шлюзу "ІІТ Захист з'єднань-2. VPN-шлюз"; програмний комплекс VPN-клієнта "ІІТ Захист з'єднань-2. VPN-клієнт". До складу апаратних засобів комплексу також можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Шлюз захисту призначений для реалізації механізмів захисту сервера та виконує наступні функції: автентифікацію клієнтів захисту при підключенні до сервера; встановлення захищеного TCP-з'єднання з клієнтом в разі успішної автентифікації; встановлення відкритого TCP-з'єднання з сервером; прийом та розшифрування даних TCP-з'єднання від клієнта та передачі їх на сервер; прийом та зашифрування даних TCP-з'єднання від сервера та передачі їх клієнту; приймання та передачу управляючої (технологічної) інформації (моніторинг захисту тощо); прийом та введення в дію ключових даних. Програмний комплекс шлюзу захисту є серверною частиною комплексу захисту з'єднань та встановлюється на окремий мережевий вузол - шлюз захисту або безпосередньо на сервер, який захищається. Шлюз захисту у вигляді апаратного засобу є окремим пристроєм та виконаний у вигляді системної платформи у металевому корпусі висотою 1U та реалізує всі функції шлюзу захисту як окремого мережевого вузла. Типи та характеристики шлюзів захисту у вигляді апаратних засобів наведені у табл. 2. Встановлення параметрів та моніторинг стану роботи шлюзу захисту у вигляді апаратного засобу здійснюється віддалено через програмний комплекс управління шлюзами. Шлюз захисту у вигляді апаратного засобу підтримує також передачу події реєстрації за протоколом syslog та видачу інформації про стан функціонування та статистику роботи за протоколом SNMP. РС адміністратора з віддаленим управлінням призначена для управління шлюзами та постійного моніторингу роботи шлюзу і виконує наступні функції: налагодження конфігурації шлюзу захисту; передачу та приймання управляючої (технологічної) інформації (стан обробки з'єднань, список активних захищених з'єднань, резервні копії конфігурації і т. ін.) у/від шлюзу захисту; генерації та завантаження ключових даних у шлюз.

Агент моніторингу призначений для отримання результатів роботи шлюзу(ів) захисту і виконує наступні функції: отримання статистики роботи шлюзу захисту; надання можливості підключення моніторами шлюзу захисту для отримання даних моніторингу. Монітор шлюзів захисту призначений для відображення результатів моніторингу роботи шлюзу(ів) захисту і виконує наступні функції: отримання та відображення статистики роботи шлюзу(ів) захисту; перегляд журналів реєстрації шлюзу захисту; сповіщення адміністратора при виявленні збоїв або відмов у роботі шлюзу. Клієнт захисту з'єднань призначений для реалізації механізмів захисту клієнтських підключень та виконує наступні функції: ініціювання процесу автентифікації клієнта на шлюзі захисту при підключенні до сервера; встановлення захищеного TCP-з'єднання зі шлюзом захисту; зашифрування даних TCP-з'єднання при передачі на сервер; розшифрування даних TCP-з'єднання при прийомі з сервера. Proxy захисту є варіантом клієнтської частини комплексу та встановлюється біля РС (ПК) кліє-

нтів. При цьому, клієнтські засоби захисту не встановлюються на РС (ПК) клієнтів. Але клієнтське програмне забезпечення повинне здійснювати підключення не до сервера, а до proxy, який буде перенаправляти їх у захищеному вигляді до сервера через шлюз захисту.

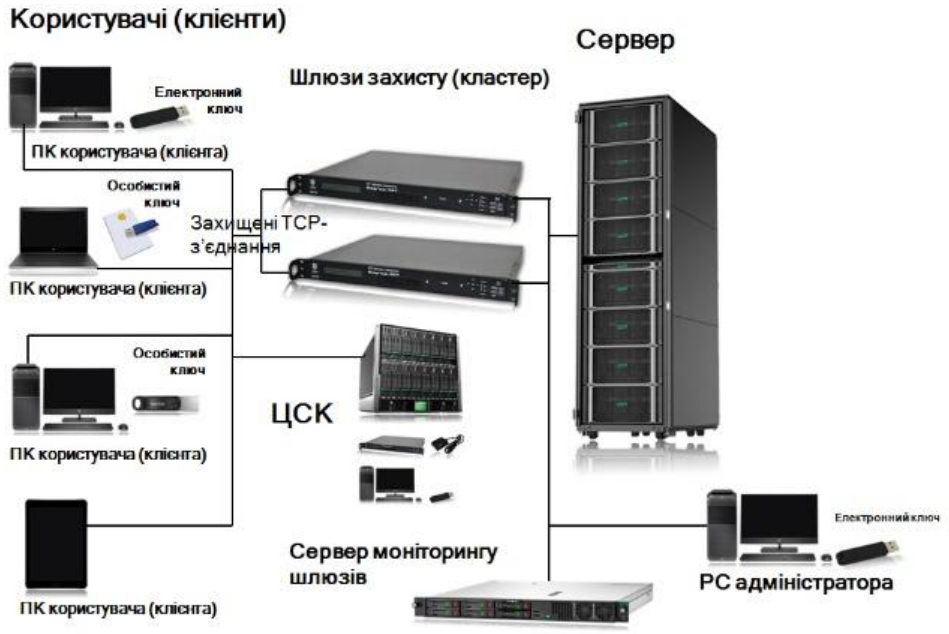


Рис. 4. Структурна схема комплексу

Таблиця 2

Типи та характеристики шлюзів захисту

Тип	Зовнішній вигляд	Інтер-фейси	Швидкість шифрування, Мбіт/с	Кількість автентифікацій клієнтів, автентифікацій/с
"Бар'єр-301" (міні-пристрій) ("ІІТ ШЗ "Бар'єр-301 (міні-пристрій)")		2 x Ethernet 100	40	10
"Бар'єр-301" (міні-пристрій) ("ІІТ ШЗ "Бар'єр-301 (міні-пристрій)")		2 x Ethernet 100/1000	125	50
"Бар'єр-301" ("ІІТ ШЗ "Бар'єр-301")		2 x Ethernet 100/1000 Опціонально – 2 x Ethernet 100/1000BASE-SX (оптичні, LC)	250	100

Монітор proxy захисту призначений для відображення результатів моніторингу роботи proxy захисту. Шлюз та клієнт захисту підтримують взаємодію клієнтських та серверних частин (клієнта та сервера) прикладних систем за протоколом TCP/IP. Під час встановлення клієнтською частиною прикладної системи TCP-з'єднання з сервером, клієнт захисту автентифікується на відповідному шлюзі захисту. Шлюз захисту при підключенні клієнта захисту проводить процедуру його автентифікації та в разі успішної автентифікації встановлює захищене TCP-з'єднання з клієнтом та відкрите TCP-з'єднання з сервером. Після проведення автентифікації (встановлення захищеного TCP-з'єднання – сеансу передачі даних) клієнт та шлюз захисту здійснюють шифрування даних (TCP-з'єднання), які передаються між клієнтом та сервером.

Клієнт захисту здійснює зашифрування даних, які відправляються від клієнта до сервера та перенаправляє їх до шлюзу, і навпаки – розшифровує дані, які приходять від сервера через шлюз.

Шлюз захисту здійснює розшифрування даних, які надходять від клієнта захисту та перенаправляє їх до сервера, і навпаки – зашифровує дані, які приходять від сервера та перенаправляє їх клієнту захисту.

VPN-шлюз призначений для реалізації механізмів створення віртуальної VPN-мережі та виконує наступні функції: створення віртуального мережевого інтерфейсу; отримання через шлюз захисту даних (MAC-кадрів) від VPN-клієнтів та передачі їх у віртуальний мережевий інтерфейс або комутації MAC-кадрів між VPN-клієнтами; отримання даних з віртуального мережевого інтерфейсу та передачі їх відповідному VPN-клієнту через шлюз захисту.

VPN-клієнт призначений для реалізації механізмів створення клієнтського підключення віртуальної VPN-мережі та виконує наступні функції: створення віртуального мережевого інтерфейсу; отримання даних (MAC-кадрів) з віртуального мережевого інтерфейсу та передачі їх на VPN-шлюз через клієнта захисту; отримання через клієнт захисту даних з VPN-шлюзу та передачі їх у віртуальний мережевий інтерфейс.

VPN-шлюз може бути інтегрований безпосередньо у шлюз захисту (програмний комплекс чи апаратний засіб). У випадку інтеграції VPN-шлюзу безпосередньо у шлюз захисту управління та моніторинг стану роботи VPN-шлюзу здійснюється шлюзом захисту. VPN-шлюз також підтримує можливість використання зовнішнього DHCP-сервера для динамічного надання VPN-клієнтам IP-адрес. У випадку інтеграції VPN-шлюзу безпосередньо у апаратний шлюз захисту, може використовуватися вбудований DHCP-сервер шлюзу захисту. Взаємодія VPN-клієнта з VPN-шлюзом здійснюється за протоколом TCP/IP. Для захисту мереженого з'єднання між VPN-клієнтом та VPN-шлюзом використовується клієнт захисту та шлюз захисту.

VPN-клієнт може також бути інтегрований безпосередньо у клієнта захисту. Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів клієнта захисту.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі програмного шлюзу захисту. Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для: автентифікації користувач (клієнта) перед початком роботи; зберігання та захисту особистого ключа користувач (клієнта); апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні клієнта.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК клієнта. Мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301") призначений для: автентифікації шлюзу захисту перед початком роботи; зберігання та захисту особистого ключа шлюзу захисту; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні шлюзу. Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до шлюзу захисту безпосередньо або через комутатори локальної обчислювальної мережі. У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12. 2012 р.

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України. Протокол встановлення захищеного сеансу передачі даних між клієнтом та шлюзом захисту реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3.

Протокол взаємної автентифікації включає: формування клієнтом та передачу даних автентифікації (запиту) на шлюз захисту; обробку запиту від клієнта шлюзом захисту; прийом та обробку відповіді клієнтом від шлюзу захисту.За результатом роботи протоколу на шлюзі захисту та клієнті встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування.

Шифрування даних у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між клієнтом та шлюзом захисту у результаті виконання протоколу взаємної автентифікації.

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані клієнтів, шлюзів захисту та адміністратора.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо. До ключових даних клієнтів, шлюзів захисту та адміністратора відносяться особисті ключі та сертифікати відповідно клієнтів, шлюзів захисту та адміністратора.

Ключові дані клієнтів, шлюзів захисту та адміністратора призначені для захисту управляючої та службової інформації при передачі між РС адміністратора та шлюзами захисту, а також для встановлення захищених з'єднань між клієнтами та шлюзами захисту та безпосередньо захисту мережевого з'єднання.

В якості носіїв ключової інформації для особистих ключів апаратних шлюзів захисту використовуються електронні ключі "Кристал-1". Шлюзи захисту також підтримують генерацію ключів безпосередньо у пристрої. Під час генерації ключів у шлюзі захисту формується запит на сертифікат, який передається у ЦСК з метою формування сертифікату. Після формування сертифікат (разом із ланцюжком сертифікатів) завантажується у шлюз захисту.

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS # 11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів клієнтів та шлюзів захисту, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів, шлюзів захисту та адміністратора; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Комплекс захисту інформації у IP-МЕРЕЖАХ "ІІТ ЗАХИСТ IP-ПОТОКУ"

Призначення комплексу: забезпечення конфіденційності та цілісності конфіденційної інформації, яка передається у розподілених системах на основі IP-мереж передачі даних.

Комплекс забезпечує: конфіденційність та цілісність інформації (мережевого IP-потоку), яка передається мережами зв'язку між розподіленими локальними обчислювальними мережами (ЛОМ) або між клієнтами та ЛОМ; організацію централізованого управління засобами захисту мережевого IP-потоку, організацію централізованої генерації та розподілу ключових даних для використання у цих засобах. Зазначені функції комплекс виконує шляхом застосування механізмів КЗІ, яка передається у вигляді мережевого IP-потоку між розподіленими ЛОМ або між клієнтами та ЛОМ через зовнішні канали зв'язку.

Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурні схеми комплексу за розміщенням його складових частин на окремих технічних засобах наведені на рис. 5 та рис. 6. IP-шифратор призначений для шифрування та контролю цілісності потоку IP-пакетів, що передаються через нього між різними ЛОМ або між клієнтами та ЛОМ і виконує такі функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу технологічної інформації (команд, поточного стану обробки потоку, резервних копій конфігурації тощо) у/від робочої станції адміністратора; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

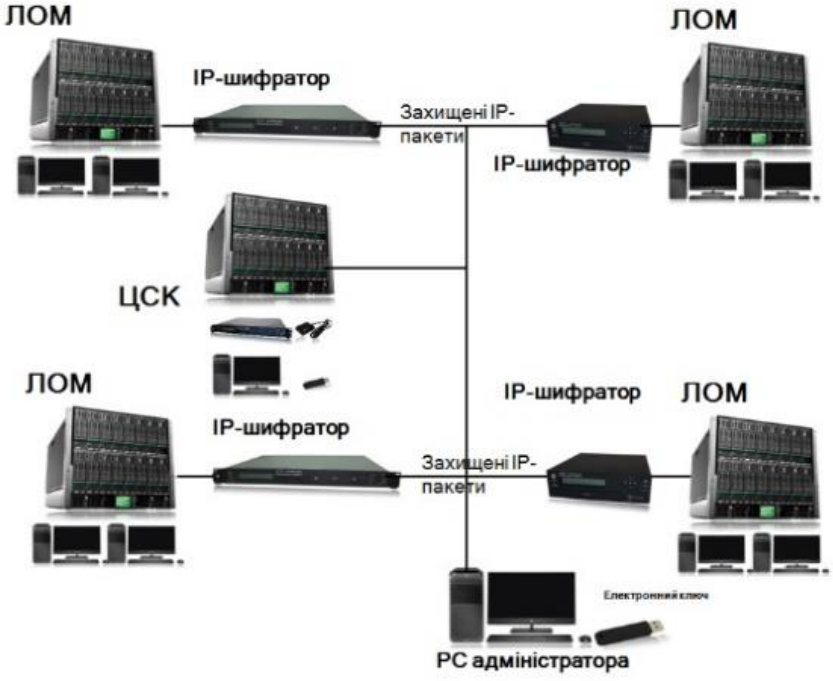


Рис. 5.Структурна схеми комплексу за розміщенням його складових частин

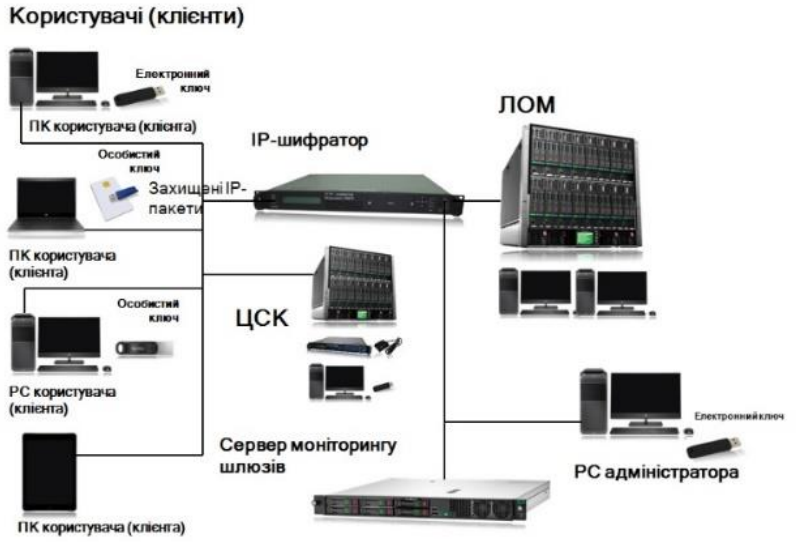


Рис. 6. Структурна схеми комплексу за розміщенням його складових частин

РС адміністратора мережі IP-шифраторів призначена для централізованого управління мережею IP-шифраторів і виконує такі функції: налагодження конфігурації кожного IP-шифратора; передачу та приймання управляючої (технологічної) інформації (стан обробки потоку, резервні копії конфігурації і т. ін.) у/від IP-шифраторів; генерації та завантаження ключових даних у IP-шифратори.

Клієнт IP-шифраторів призначений для шифрування та контролю цілісності потоку IP-пакетів, що передаються між ним та IP-шифратором(ами) і виконує такі функції: встановлення захищених з'єднань з IP-шифраторами; шифрування та контроль цілісності IP-пакетів.

IP-шифратори виконують шифрування та контроль цілісності потоків мережних IP-пакетів, що передаються через них між розподіленими ЛОМ або між клієнтами та ЛОМ.

Для забезпечення транзитної передачі даних IP-шифратори мають два мережних інтерфейси типу Ethernet – внутрішні та зовнішні. До внутрішніх інтерфейсів підключається комунікаційне обладнання ЛОМ, а зовнішні підключаються до зовнішньої мережі передачі даних.

IP-пакети, отримані через внутрішні мережні інтерфейси із ЛОМ зашифровуються та захищаються контрольною сумою і маршрутизуються на зовнішній інтерфейс для передачі через зовнішній мережі. IP-пакети, отримані через зовнішні інтерфейси із зовнішньої мережі розшифровуються та перевіряються на цілісність і маршрутизуються на внутрішній інтерфейс для передачі у ЛОМ.

IP-шифратори підтримують захист IP-потоку для повнозв'язної топології ЛОМ ("кожний з кожним").

Віддалене управління IP-шифраторами з РС адміністратора здійснюється через мережі передачі даних з підключенням до одного з інтерфейсів.

IP-шифратори, що входять до складу комплексу, функціонують у автоматизованому режимі з віддаленим управлінням з РС адміністратора.

Комплекс забезпечує характеристики, що наведені у табл. 3. Типи та характеристики IP-шифраторів наведені у табл. 4.

Таблиця 3

Характеристики комплексу

Характеристика	Значення
Кількість захищених з'єднань IP-шифраторів	не менше 1024 з'єднань (зв'язок IP-шифратора з 1024 іншими)
Кількість захищених з'єднань з клієнтами	не менше 4096 з'єднань (зв'язок IP-шифратора з 4096 клієнтами)
Швидкість обробки IP-потоку (захисту)	не менше 25 Мбіт/с (до 450 Мбіт/с)
Кількість IP-шифраторів, якими управляє один адміністратор мережі	не менше 1024

У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування). Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р.

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку.

Протокол встановлення захищеного сеансу передачі даних між IP-шифраторами або між клієнтом та IP-шифратором реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3. Протокол взаємної автентифікації включає: формування ініціатором (IP-шифратором чи клієнтом) та передачу даних автентифікації (запиту) на IP-шифратор; обробку запиту IP-шифратором; прийом та обробку відповіді ініціатором від IP-шифратора. За результатом роботи протоколу на IP-шифраторах чи IP-шифраторі та клієнті встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування IP-пакетів у дуплексному режимі.

Таблиця 4

Типи та характеристики IP-шифраторів

Тип	Зовнішній вигляд	Інтерфейси	Швидкість шифрування, Мбіт/с
"Канал-201" (мікро-пристрій) ("ІІТ IP-шифратор Канал-201 (мікро-пристрій)")		USB (RNDIS), Ethernet 10/100	40
"Канал-201" ("ІІТ IP-шифратор Канал-201")		2 x Ethernet 100/1000	125
"Канал-301" ("ІІТ IP-шифратор Канал-301")		2 x Ethernet 100/1000, опціонально - 2 x Ethernet 100/1000BASE-SX (оптичні, LC)	1000 (1 Гбіт/с)
"Канал-401" ("ІІТ IP-шифратор Канал-401")		2 x Ethernet 100/1000, 2 x SFP+ (1000/10000, оптичні SFP-модулі 1000BASE-SX, 10G-SR чи ін.)	5000 (5 Гбіт/с)

Шифрування IP-пакетів здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування. Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані IP-шифраторів, адміністратора та клієнтів. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо. До ключових даних IP-шифраторів, адміністратора та клієнтів відносяться особисті ключі та сертифікати відповідно IP-шифраторів, адміністратора та клієнтів. Ключові дані IP-шифраторів, адміністратора та клієнтів призначені для захисту управляючої та службової інформації при передачі між РС адміністратора та IP-шифраторами, а також для встановлення захищених з'єднань між IP-шифраторами або між клієнтами та IP-шифраторами та безпосередньо захисту IP-потоку.

В якості носіїв ключової інформації для особистих ключів IP-шифраторів використовуються електронні ключі "Кристал-1" ("ІІТ Е.ключ Кристал-1"). IP-шифратори також підтримують генерацію ключів безпосередньо у пристрої. Під час генерації ключів у IP-шифраторі формується запит на сертифікат, який передається у ЦСК з метою формування сертифікату. Після формування сертифікат (разом із ланцюжком сертифікатів) завантажується у IP-шифратор. IP-шифратори також підтримують генерацію ключів безпосередньо у пристрої.

Під час генерації ключів у IP-шифраторі формується запит на сертифікат, який передається у ЦСК з метою формування сертифікату. Після формування сертифікат завантажується у IP-шифратор. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"); інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус

сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12. Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів IP-шифраторів, адміністратора та клієнтів, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів. Програмно-технічний комплекс (ПТК) СК забезпечує: обслуговування сертифікатів IP-шифраторів, адміністратора та клієнтів, що включає: надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів.

Комплекс захисту інформації на носіях "ІІТ ЗАХИЩЕНИЙ ДИСК-4"

Призначення комплексу: забезпечення конфіденційності інформації, яка зберігається на носіях інформації робочих станцій, портативних комп'ютерів та серверів (жорстких дисках, електронних flash-дисках, картах пам'яті тощо) з використанням механізмів та засобів КЗІ. Структурна схема комплексу наведена на рис. 7.

До складу комплексу входять: програмний комплекс захисту інформації на носіях користувача "ІІТ Захищений диск-4. Користувач"; програмний комплекс захисту інформації на носіях сервера "ІІТ Захищений диск-4. Сервер". До складу апаратних засобів комплексу також може входити електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"). Програмні засоби комплексу забезпечують захист інформації на носіях інформації робочих станцій (РС) та серверів (жорстких дисках, електронних flash-дисках, картах пам'яті тощо).

Захист інформації забезпечується прозорим шифруванням областей дискового простору чи створенням віртуальних логічних дисків, які фізично є зашифрованими областями дисків чи файлами-образами.

Засоби захисту носіїв серверів підтримують автоматичне підключення захищених дисків, аварійне відключення та знищення захищених дисків, забезпечення доступу до них з ЛОМ та ін.

Засоби захисту носіїв портативних комп'ютерів забезпечують шифрування даних на вбудованих та на зовнішніх картах пам'яті. Програмні засоби комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі тощо.

Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для апаратної реалізації криптографічних перетворень усередині пристрою та реалізує: автентифікацію користувача перед початком роботи; зберігання та захист особистого ключа користувача.

Електронний ключ має електричний USB-інтерфейс для підключення. У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Рис. 7. Структурна схема комплексу "Електронний ключ"

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України. Шифрування секторів захищених дисків виконується в двох режимах: спочатку в режимі простої заміни, а потім в режимі гамування із зворотнім зв'язком згідно ДСТУ ГОСТ 28147:2009.

Шифрування здійснюється на ключі шифрування диску, який зберігається разом із диском. Захист ключа шифрування диску виконується на ключі захисту, який отримується шляхом гешування за ГОСТ 34.311-95 особистого ключа протоколу розподілу ключів.

Довгострокові ключові елементи (ДКЕ) для алгоритму шифрування ДСТУ ГОСТ 28147:2009 постачаються відповідно до вимог Держспецзв'язку України. До ключових даних комплексу відносяться особисті ключі користувачів і серверів, що використовують захищені диски. В якості особистих ключів можуть використовуватися особисті ключ користувачів центру сертифікації ключів (ЦСК, при цьому, в якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1").

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів (формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12).

Комплекс захисту SAP-системи "ІІТ ЗАХИСТ SAP"

Повна назва комплексу: комплекс захисту SAP-системи "ІІТ Захист SAP". Призначення комплексу: криптографічний захист інформації у SAP-системі, а саме: автентифікація користувачів SAP-системи та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером системи, з використанням механізмів КЗІ; забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК).

Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рис. 8.До складу комплексу входять: програмний комплекс захисту SAP-клієнта "ІІТ Захист SAP. Клієнт"; програмний комплекс захисту SAP-сервера "ІІТ Захист SAP. Сервер"; програмний комплекс віддаленого моніторингу захисту SAP-сервера "ІІТ Захист SAP. Віддалений монітор сервера". До складу апаратних засобів можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301"). Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у клієнтську та серверну частини SAP-системи (SAP-клієнта та SAP-сервер), через визначені у SAP-системі механізми та інтерфейси КЗІ.

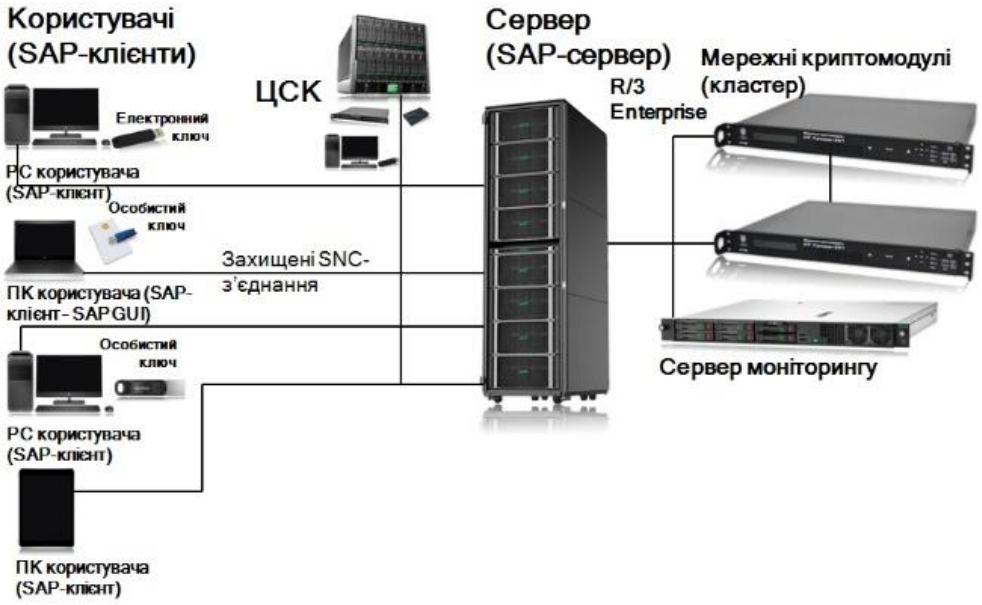


Рис. 8. Структурна схема комплексу

Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо. SNC-бібліотеки (бібліотеки захисту з'єднань) у складі SAP-клієнта та SAP-сервера призначені для реалізації механізмів автентифікації користувачів SAP-системи на сервері під час підключення користувачів до сервера (встановлення з'єднання з сервером), шляхом реалізації протоколу взаємної автентифікації сторін, та забезпечення конфіденційності і цілісності інформації, яка передається між користувачами та сервером SAP-системи під час їх взаємодії, шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Протокол взаємної автентифікації сторін (встановлення захищеного з'єднання) включає наступні шаги (етапи): формування та передачу запиту від користувача SAP-системи на сервер; обробку запиту від користувача сервером (що включає, в тому числі, перевірку чинності сертифіката користувача), формування та відправку відповіді за результатами обробки запиту; прийом та обробку відповіді від сервера користувачем та прийняття рішення про успішність встановлення захищеного з'єднання (що аналогічно включає і перевірку чинності сертифіката сервера).

SSF-бібліотека (бібліотека захищеного зберігання та пересилання) у складі SAP-клієнта та SAP-сервера призначена для забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у SAP-системі, шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача SAP-системи, так і на стороні сервера.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання SNC- та SSF-бібліотеками в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС); зашифрування та розшифрування даних; формування та перевірку ЕЦП від даних; захист сеансів передачі даних (захист з'єднань); інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК); отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Засоби управління та моніторингу стану захисту клієнта призначені для встановлення параметрів

SNC- та SSF-бібліотек, параметрів бібліотеки користувача ЦСК, а також моніторингу та відображення стану їх роботи. Засоби управління захистом сервера призначені для встановлення параметрів SNC- та SSF-бібліотек, а також параметрів бібліотеки користувача ЦСК.

Агент моніторингу захисту SAP-сервера призначений для зберігання інформації про стан та статистику функціонування програмних засобів захисту сервера (списку активних захищених з'єднань SNC-бібліотеки тощо), а також ведення журналів реєстрації подій та надання доступу до цієї інформації засобам віддаленого моніторингу. Інформацію про стан та статистику функціонування до агента моніторингу передають SNC- та SSF-бібліотеки.

Програмний комплекс віддаленого моніторингу захисту SAP-сервера призначений для отримання від агента моніторингу сервера та відображення інформації про стан і статистику функціонування програмних засобів захисту та подій з журналів реєстрації.

SNC-бібліотеки (бібліотеки захисту з'єднань) реалізовані у відповідності до визначених розробником SAP-системи специфікацій програмних інтерфейсів: інтерфейсу GSS-API v2, який реалізує всі механізми КЗІ згідно з міжнародними технічними рекомендаціями RFC-2078; інтерфейс SNC-адаптера, який визначений у внутрішньому технічному документі компанії SAP та призначений для безпосередньої інтеграції бібліотеки у SAP-клієнт та SAP-сервер, і є проміжним інтерфейсом між GSS-API v2 та SAP-системою. SSF-бібліотеки (бібліотеки захищеного зберігання та пересилання) реалізовані у відповідності до визначеної розробником SAP-системи специфікації програмного інтерфейсу SSF-API. Зазначений інтерфейс визначений у внутрішньому технічному документі компанії SAP.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі користувача SAP-системи. Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера SAP-системи.

Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для: автентифікації користувача SAP-системи перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача SAP-системи.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача SAP-системи.

Мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301") призначений для: автентифікації сервера SAP-системи перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера SAP-системи.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до сервера SAP-системи безпосередньо або через комутатори локальної обчислювальної мережі. Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку сервера SAP-системи. У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України. Протокол встановлення захищеного сеансу передачі даних між SAP-клієнтом та SAP-сервером реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3.

За результатом роботи протоколу на сервері та клієнті встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування. В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з'єднанні використовуються імітовставки, які обчислюються за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі вироблення імітовставки.Шифрування даних та обчислення імітовставок у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між клієнтом та сервером у результаті виконання протоколу взаємної автентифікації.

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та сервера SAP-системи. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера SAP-системи відносяться особисті ключі та сертифікати відповідно користувачів та сервера.

В якості носіїв ключової інформації для особистих ключів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301";

інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів користувачів та сервера; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Засоби електронного цифрового підпису (ЕЦП) для платформи ORACLE FLEXCUBE "ІІТ ЕЦП ДЛЯ ORACLE FLEXCUBE".

Призначення засобів: забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у платформі, з використанням електронного цифрового підпису.

Зазначені функції засоби виконують шляхом застосування механізмів ЕЦП. Для організації ключової системи (управління ключовими даними) засобів використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурна схема засобів за розміщенням їх складових частин на окремих технічних засобах наведена на рис. 9.

До складу засобів входять: засоби ЕЦП для FlexCube-клієнта у складі бібліотеки користувача ЦСК для web-оглядача "ІІТ Користувач ЦСК-1. Бібліотека FlexCube (Active-X)" (Active-X-бібліотека ЕЦП), яка включає бібліотеку користувача ЦСК "ІІТ Користувач ЦСК-1. Бібліотека підпису"; програмний комплекс сервера ЕЦП для FlexCube-сервера у складі: програмний комплекс віддаленого моніторингу бібліотек користувача ЦСК "ІІТ Користувач ЦСК-1. Віддалений моніторинг бібліотек".

До складу апаратних засобів можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") чи електронний ключ "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Програмні засоби ЕЦП реалізують логіку роботи засобів та інтегровані безпосередньо у клієнтську та серверну частини платформи Oracle FlexCube (FlexCube-клієнта та FlexCube-сервер), через визначені у платформі Oracle FlexCube механізми та інтерфейси ЕЦП.

Програмні засоби КЗІ можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо.

Active-X-бібліотека ЕЦП у складі FlexCube-клієнта, який виконується безпосередньо у web-оглядачі, призначена для забезпечення цілісності та неспростовності авторства електронних даних та документів, що обробляються клієнтом (користувачем), шляхом формування та перевіряння ЕЦП від даних та документів на стороні клієнта.

Рис. 9. Структурна схема комплексу

Web-служба ЕЦП у складі сервера ЕЦП, який підключений до FlexCube-сервера та доступний за протоколом SOAP, призначена для забезпечення цілісності та неспростовності авторства електронних даних та документів, що обробляються FlexCube-сервером, шляхом формування та перевіряння ЕЦП від даних та документів на стороні сервера.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання Active-X-бібліотекою та web-службою ЕЦП в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС); зашифрування та розшифрування даних; формування та перевірку ЕЦП від даних; захист сеансів передачі даних (захист з'єднань); інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК); отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Програмний комплекс віддаленого моніторингу бібліотек користувача ЦСК призначений для отримання від агента моніторингу бібліотек та відображення інформації про стан і статистику функціонування програмних засобів та подій з журналів реєстрації.

Зберігання інформації про стан та статистику функціонування програмних засобів, а також ведення журналів реєстрації подій та надання доступу до цієї інформації засобам віддаленого моніторингу здійснює агент моніторингу бібліотек. Інформацію про стан та статистику функціонування до агента моніторингу передають бібліотеки користувача ЦСК.

Active-X-бібліотека ЕЦП реалізована у вигляді Active-X-об'єкту у відповідності до визначених розробником платформи Oracle FlexCube специфікацій програмних інтерфейсів та доступна FlexCube-клієнту через виклики JavaScript-функції.

Web-служба ЕЦП реалізована у відповідності до визначеної розробником платформи Oracle Flex Cube специфікацій та доступна FlexCube-серверу за протоколом SOAP через java-модулі (JAX-WS) чи PL/SQL-модулі.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі користувача платформи Oracle FlexCube. Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера платформи Oracle FlexCube. Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для: автентифікації користувача платформи Oracle FlexCube перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача платформи.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача платформи Oracle FlexCube.

Мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301") призначений для: автентифікації сервера ЕЦП перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера ЕЦП.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до сервера ЕЦП безпосередньо або через комутатори локальної обчислювальної мережі. Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку сервера ЕЦП.

У засобах використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147: 2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р.

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку. Організацію ключової системи засобів виконує центр сертифікації ключів (ЦСК).

У засобах використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та сервера ЕЦП. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера ЕЦП відносяться особисті ключі та сертифікати відповідно користувачів та сервера.

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS# 11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог

до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів користувачів та сервера; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Засоби захисту входу в контролер домену MICROSOFT ACTIVE DIRECTORY "ІІТ ЗАХИЩЕНИЙ ВХІД"

Призначення засобів: автентифікація користувачів операційних систем (ОС) Microsoft Windows в контролері домену Microsoft Active Directory при вході в ОС та при доступі до ресурсів.

Зазначені функції засоби виконують шляхом застосування механізмів КЗІ.

Автентифікація користувачів в контролері домену здійснюється під час входу користувача до ОС з його робочій станції (РС) чи портативному комп'ютері (ПК) з використанням апаратних засобів КЗІ (носіїв ключової інформації) користувача, таких як електронні ключі та смарт-карти. Для організації ключової системи (управління ключовими даними) засобів користувачів та контролера домену використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурна схема засобів за розміщенням їх складових частин на окремих технічних засобах наведена на рис. 10.

Рис. 10. Структурна схема комплексу

До складу засобів входять програмні засоби інтеграції носіїв ключової інформації (в т.ч. і апаратних засобів КЗІ) користувачів в ОС - програмний комплекс захисту входу користувача "ІІТ Захищений вхід. Користувач" для ОС Microsoft Windows, який включає: міні-драйвери смарт-карт носіїв ключів (як апаратних засобів КЗІ так і віртуальних); віртуального драйвера смарт-карт; програмних засобів (бібліотек) КЗІ (користувача ЦСК) "ІІТ Користувач ЦСК-1".

До складу апаратних засобів КЗІ користувачів можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); електронний ключ "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"); смарт-карта "Карта-1" ("ІІТ Смарт-карта Карта-1").

Програмні засоби інтегруються безпосередньо у підсистему автентифікації ОС на стороні користувача контролеру домену Microsoft Active Directory.

Програмні засоби для автентифікації на контролері домену можуть використовувати зовнішні апаратні засоби КЗІ (носії ключової інформації) користувача, такі як електронні ключі та смарт-карти.

Міні-драйвер смарт-карт призначений для інтеграції апаратних засобів КЗІ (носіїв ключової інформації) у підсистему автентифікації ОС на стороні користувача та забезпечення розпізнавання апаратних засобів у підсистемі автентифікації ОС та їх використання в процесі автентифікації на контролері домену.

Віртуальний драйвер смарт-карт використовуються для носіїв ключової інформації та апаратних засобів КЗІ (наприклад, електронних ключів), які не є смарт-картами та потребують емуляції поведінки смарт-карти у ОС з метою їх розпізнавання ОС на стороні користувача в якості смарт-карти.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання мінідрайвером смарт-карт в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв) та взаємодію з апаратними засобами КЗІ); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС); інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК) тощо.

Електронні ключі, смарт-карти чи інші носії ключової інформації (апаратні засоби КЗІ) призначені для зберігання особистого ключа автентифікації користувача на контролері домену. Програмні засоби інтеграції носіїв ключової інформації (апаратних засобів КЗІ) користувачів в ОС встановлюються та використовуються виключно на стороні користувача на його РС (ПК). Для автентифікації користувачів на контролері домену (сервері) має бути налаштована служба Microsoft Active Directory та створений і налаштований домен, а користувачі, які мають автентифікуватися в контролері, повинні бути користувачами створеного домену. На контролері домену не здійснюється встановлення жодних складових частин засобів.

В якості ОС користувачів, в які інтегровано засоби автентифікації, можуть використовуватися ОС Microsoft Windows XP/ Vista/7/8/8.1/10. В якості ОС контролера домену (сервера) можуть використовуватися ОС Microsoft Windows 2003/2008/2012/ 2016/2019 Server. У засобах використовуються такі криптографічні алгоритми та протоколи: алгоритми шифрування TDEA і AES за ISO/IEC 18033-3:2010; алгоритм ЕЦП RSA за PKCS# 1 (RFC 3447); алгоритми гешування SHA (SHA-1 і SHA-224/256/384/512) за ДСТУ ISO/IEC 10118-3:2005; протокол розподілу клю-

чів RSA за PKCS#1 (RFC 3447). Автентифікація користувача на контролері домену здійснюється за протоколом Kerberos, який реалізований штатними засобами ОС користувача та контролера домену. Під час автентифікації штатні засоби ОС користувача здійснюють звертання (використовують) міні-драйвер смарт-карт для виконання криптографічних перетворень.

У засобах використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та контролера домену. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів тощо. До ключових даних користувачів та контролера домену відносяться особисті ключі та сертифікати відповідно користувачів та контролера домену. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та контролера домену, а також надання (за необхідності) користувачам і контролеру домену засобів генерації особистих та відкритих ключів. Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів користувачів та контролера домену; надання користувачам та контролеру домену (за необхідності) засобів генерації особистих та відкритих ключів. Для взаємодії з центром сертифікації ключів (використання його інтерактивних служб) користувачі та контролер домену повинні мати можливість мережевого підключення до ЦСК. Усі механізми взаємодії з ЦСК виконують бібліотеки користувача ЦСК. Зміна статусу сертифікатів (блокування, поновлення або скасування) та знищення особистих ключів користувачів та контролера домену здійснюється у відповідності до порядку, який визначений ЦСК (згідно регламенту ЦСК).

В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1". Далі наведемо розроблені і впроваджені апаратні засоби КЗІ.

Електронний ключ "Кристал-1Д"

Засіб (див. рис. 11) виконує наступні функції: автентифікацію оператора ЕОМ при доступі до ключа; генерацію ключів; зберігання ключів у внутрішній пам'яті та захист їх від НСД; формування і перевірку ЕП; розподіл ключових даних та шифрування даних; зберігання довільних даних у внутрішній пам'яті та захист їх від НСД; контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

Рис. 11. Електронний ключ "Кристал-1Д"

Засіб призначений для захисту службової інформації. Електронний ключ виконаний у вигляді малогабаритного знімного USB-пристрою. Конструктивно електронний ключ виконаний на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар та встановлена у металевий корпус, що формує зовнішній вигляд засобу. На друкованій платі встановлюються електроні компоненти та USB-з'єднувач типу A-plug (виделка). Швидкість формування ЕП – 100 мс. Швидкість розподілу ключових даних – 800 мс. Швидкість шифрування – 800 Кбіт/с.

IP-шифратор "Канал-101ДЕ"

IP-шифратор (див. рис. 12) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

Рис. 12. Р-шифратор "Канал-101ДЕ"

Засіб призначений для захисту службової інформації. IP-шифратор виконаний у вигляді окремого малогабаритного мережевого пристрою. Конструктивно IP-шифратор є мініатюрною системною платформою у металевому корпусі та має 2 мережних інтерфейси Ethernet 100Base-TX. Швидкість шифрування – не менше 30 Мбіт/с (до 40 Мбіт/с).

IP-шифратор "Канал-201Д"

IP-шифратор (див. рис. 13) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та

введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами. Засіб призначений для захисту службової інформації. IP-шифратор виконаний у вигляді окремого мережевого вузла.

Рис. 13. IP-шифратор "Канал-201Д"

Конструктивно IP-шифратор є системною платформою у металевому корпусі висотою 2U та може встановлюватись в 19-ти дюймову стійку за допомогою полки. Засіб має 2 дуплексні оптичні мережні інтерфейси Ethernet 100Base-SX (тип роз'єму - FC). Засіб має систему спеціального захисту від витоку інформації каналами ПЕМВН. Швидкість шифрування - не менше 75 Мбіт/с (до 100 Мбіт/с).

IP-шифратор "Канал-301Д"

IP-шифратор (див. рис. 14) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

Засіб призначений для захисту службової інформації. IP-шифратор виконаний у вигляді окремого мережевого вузла.

Рис. 14. IP-шифратор "Канал-301Д"

Конструктивно IP-шифратор є системною платформою у металевому корпусі висотою 2U та призначену для встановлення в 19-ти дюймову стійку. Засіб має 2 дуплексні оптичні мережні інтерфейси Ethernet 1000Base-SX (тип роз'єму - FC). Засіб має систему спеціального захисту від витоку інформації каналами ПЕМВН. Швидкість шифрування – не менше 350 Мбіт/с (до 1 Гбіт/с).

IP-шифратор "Канал-401Д"

IP-шифратор (див. рис. 15) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами. IP-шифратор виконаний у вигляді окремого мережевого вузла. Конструктивно IP-шифратор є системною платформою у металевому корпусі висотою 2U та призначену для встановлення в 19-ти дюймову стійку. Засіб має 2 дуплексні оптичні мережні інтерфейси Ethernet 10GBASE-SR (тип роз'єму - FC). Засіб має систему спеціального захисту від витоку інформації каналами ПЕМВН. Швидкість шифрування – не менше 5 Гбіт/с (до 15 Гбіт/с).

Рис. 15. IP-шифратор "Канал-401Д"

АС «Оберіг» Міністерства оборони України

Комплекси КЗІ, які побудовані з використанням IP-шифратор Канал-101ДЕ та Канал-301Д, входять до складу спеціального забезпечення та віддаленого управління «ІІТ захист IP-потоку-2Д.

Віддалене управління IP-шифраторами», що є основними складовими елементами захисту інформації автоматизованої інформаційно-телекомунікаційній системи «Оберіг» (далі – АС «Оберіг»).

Комплекс КЗІ АС «Оберіг» призначений для збирання, зберігання, обробки та використання даних про військовозобов'язаних (призовників), створена для забезпечення військового обліку громадян України та на теперішний час охоплюють понад 600 мереж спеціального призначення.

АС «Оберіг» створено та розгорнуто у відповідності до Закону України № 1951-VIII від 16 березня 2017 року «Про Єдиний державний реєстр військовозобов'язаних», Концепції військової кадрової політики у ЗС України на період до 2020 року (затверджена наказом Міністерства оборони України № 342 від 26.06.2017) та є одною зі складових розвитку військової кадрової політики – впровадження єдиної автоматизованої інформаційно-аналітичної системи обліку та управління персоналом до окремої військової частини та застосовування її у повсякденній діяльності служб персоналу. АС «Оберіг» впроваджено та стало функціонує у: кадрових органах ЗС України верхнього рівня, які здійснюють функції управління персоналом (Департаменті кадрової політки МО України, Головному управлінні персоналом ГШ ЗС України, Кадровому центрі ГШ ЗС України), та середнього рівня (управління персоналу та Кадрові центри видів ЗС України) та об'єднує дані від систем, які вже працюють у ЗС або будуть створюватись. АС «Оберіг» має потужний механізм для аналітичного опрацювання всієї інформації, яка вноситься до загальних баз даних, та можливість відображати данні у зручній наочній формі.

Крім того, АС «Оберіг» має низку переваг, а саме: є можливість створювати аналітичні звіти; до підсистеми закладено потужний пошуковий механізм за всіма типами даних, що внесені до баз даних; забезпечено цілісність та повноту накопиченої інформації; унеможливлено багаторазове введення даних та наявність розбіжностей в них; розширені можливості для створення і здійснення не тільки звітності, але й смартформ (бланків, що автоматично заповнюються на основі запитів); ведення документообігу. Окремі елементи АС «Оберіг» встановлено та використовується у:

Міністерство оборони України; Генеральному штабі Збройних Сил України; обласні військові комісаріати та оперативні командування (у межах повноважень за військово-адміністративним поділом території України); районні (міські) військові комісаріати.

Спеціальна інформаційно-телекомунікаційна система Національної системи конфіденційного зв'язку

Спеціальна інформаційно-телекомунікаційна система органів виконавчої влади є складовою Національної системи конфіденційного зв'язку (СІТС НСКЗ) створено відповідно до Закону України від 10.01.2020 № 2919-III «Про Національну систему конфіденційного зв'язку» та Розпорядження Кабінету Міністрів України від 11.06.2003 № 338-р «Про створення спеціальної інформаційно-телекомунікаційної системи органів виконавчої влади» з метою побудови спеціальної інформаційно-телекомунікаційної системи органів виконавчої влади та забезпечення циркуляції інформації з обмеженим доступом, крім інформації, що становить державну таємницю, в інтересах органів державної влади та органів місцевого самоврядування, юридичних та фізичних осіб незалежно від форми власності, створюються належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.

Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям встановлюється Кабінетом Міністрів України (постанова КМУ від 11.10.2002 №1519 «Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям»).

Головним виконавцем робіт із створення СІТС НСКЗ визначено державне підприємство «Українські спеціальні системи» (далі – ДП «УСС») яка виконує роботи із створення абонентських пунктів СІТС НСКЗ із використанням криптографічного захисту службової інформації IP-шифратор «Канал-101ДЕ», IP-шифратор «Канал-201Д» та IP-шифратор «Канал-301Д» та їх підключення до головного комутаційного центру.

На сьогодні ДП «УСС» є провідним надавачем послуг конфіденційного зв'язку, у тому числі надання у користування захищених каналів передачі даних, захищеного доступу до Інтернету органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним особам у мережі НСКЗ.

Засоби КЗІ на базі IP-шифраторів «Канал-101ДЕ», «Канал-201Д» та «Канал-301Д» використовуються для забезпечення функціонування абонентських пунктів СІТС НСКЗ та організації захищеного каналу зв'язку для доступу автоматизованих робочих місць в багатьох міністерствах та відомствах України та на теперішній час охоплюють понад 2 000 мереж спеціального призначення.

Захищена телекомунікаційна мережа Державної міграційної служби України

На виконання вимог Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» та відповідно до «Плану заходів із запровадження документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, у які імплантовано безконтактний електронний носій, і створення національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства на 2014 - 2017 роки», затвердженого розпорядженням Кабінету Міністрів України від 20 серпня 2014 р. № 780-р, проведено роботи з розгортання в територіальних органах Державної міграційної служби України та їх підрозділах захищеної телекомунікаційної мережі шляхом встановлення відповідного обладнання та організації захищених каналів зв'язку.

Для організації захищених каналів зв'язку використовується обладнання криптографічного захисту службової інформації IP-шифратор «Канал-101ДЕ», IP-шифратор «Канал-201Д» та IP-шифратор «Канал-301Д» виробництва Приватного акціонерного товариства «Інститут інформаційних технологій» (АТ «ІІТ»).

Висновки

В роботі реалізовано проекти з розробки та впровадження програмно-технічних комплексів та апаратних засобів КЗІ для надавачів електронних довірчих послуг Збройних сил України, Міністерства внутрішніх справ, Державної прикордонної служби, Державної податкової служби України, Національного банку України, Приватбанку, Укрсіббанку, Альфа банку тощо, всього – 17 комплексів, включно по два технологічні центри сертифікації ключів для Центрального засвідчувального органу України та засвідчувального центру Національного банку України. Таким чином, розроблені програмно-технічні комплекси та апаратні засоби КЗІ створили безпечне пост-квантове довкілля для державних електронних інформаційних ресурсів.

Література

[1]. О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, Ю.І. Горбенко. *Потокові шифри. Монографія*. Під загальною редакцією І.Д. Горбенка. Х.: Форт, 2019.- 541 с.

[2]. *ISCI'2017: Information Security in Critical Infrastructures*. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017.–207 p.

[3]. Паціра Є.В. *Энциклопедия безопасности авиации* / Кулик М.С., Харченко В.П., Корченко О.Г. // Монографія. – К.: Техника, 2008. – 1000 с.

[4]. Корченко А.О. *Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія*, Київ, ЦП «Компринт», 2019. – 361 с.

[5]. Zadiraka V. Spectral methods of computer steganography problem decision / V. Zadiraka, N. Koshkina // *Methods of effective protection of information flows*. – Ternopil: Terno-graf, 2014. – Ch. 4. – pp. 96–120.

[6]. А. Корченко, Є. Іванченко, Н. Кошкіна, О. Кузнецов, О. Качко, О. Потій, В. Онопрієнко, В. Бобух. Стандартизація систем, комплексів та засобів КЗІ для застосування у пост-квантовому довкілі. *Захист інформації*. Том 22, № 4. К.: НАУ, 2020, С. 227-262.

УДК 004.056

Корченко А.А., Иванченко Е.В., Кошкина Н.В., Кузнецов А.А., Качко Е.Г., Потый А.В., Оноприенко В.В., Бобух В.А. Современные комплексы пост-квантовой безопасности государственных электронных информационных ресурсов.

Аннотация. В настоящее время в условиях широкого внедрения цифровых технологий в экономическую, оборонную сферы и сферу безопасности, во всех ведущих странах мира остро стоит проблема обеспечения безопасности их киберпространства, особенно в условиях новых угроз, порождаемых использованием квантовых компьютеров. Поэтому создание в Украине соответствующей системы безопасности киберпространственной окружающей среды национальной критической информационной инфраструктуры, в частности комплексов и средств обнаружения вторжений, криптографической и стеганографической защиты информации, является современной и актуальной проблематикой, которая непосредственно касается пост-квантовой информационной и кибербезопасности нашего государства, а также имеет важное общегосударственное и оборонное значение и существенно влияет на обеспечение национальной безопасности Украины в условиях ведения информационных и гибридных войн. Исходя из актульности проблемы обеспечения национальной безопасности Украины в условиях ведения информационных и гибридных войн, целью работы является совершенствование систем специального назначения за счет построения комплексов криптографической защиты информации пост-квантовой безопасности государственных электронных информационных ресурсов. В работе реализованы проекты по разработке и внедрению программно-технических комплексов и аппаратных средств криптографической защиты информации для поставщиков электронных доверительных услуг Вооруженных сил Украины, Министерства внутренних дел, Государственной пограничной службы, Государственной налоговой службы Украины, Национального банка Украины, Приватбанка, УкрСиббанка, Альфа банка и т.д., включительно по два технологических центра сертификации ключей для Центрального удостоверяющего органа Украины и удостоверяющего центра Национального банка Украины. Таким образом, разработанные программно-технические комплексы и аппаратные средства криптографической создали безопасную пост-квантовую окружающую среду для государственных электронных информационных ресурсов.

Ключевые слова: сетей передачи данных специального назначения, криптографические средства, комплексы специального назначения, средства защиты информации, киберпространство, пост-квантовая окружающая среда, государственные электронные информационные ресурсы.

Korchenko A., Ivanchenko Ye., Koshkina N., Kuznetsov O., Kachko O., Potiy O., Onoprienko V., Bobukh V. Modern developed of post-quantum safety of state-owned electronic information resources.

Abstract. Currently, in the context of the widespread introduction of digital technologies in the economic, defense and security spheres, in all the leading countries of the world there is an acute problem of ensuring the security of their cyberspace, especially in the context of new threats generated by the use of quantum computers. Therefore, the creation in Ukraine of an appropriate security system for the cyberspace environment, national critical information infrastructure, in particular intrusion detection systems and tools, cryptographic and steganographic information protection, is a modern and topical issue that directly concerns the post-quantum information and cybersecurity of our state, and also has an important national and defense significance and significantly affects the national security of Ukraine in the context of information and hybrid wars. Proceeding from the urgency of the problem of ensuring the national security of Ukraine in the context of information and hybrid wars, the aim of the work is to improve special purpose systems by building complexes of cryptographic information protection of post-quantum security of state electronic information resources.The work has implemented projects for the development and implementation of software and hardware systems and hardware cryptographic protection of information for providers of electronic trust services of the Armed Forces of Ukraine, the Ministry of Internal Affairs, the State Border Guard Service, the State Tax Service of Ukraine, the National Bank of Ukraine, Privatbank, UkrSibbank, Alfa Bank, etc., including two technological and logical centers for certification of keys for the Central Certification Authority of Ukraine and the Certification Center of the National Bank of Ukraine. Thus, the developed software and hardware systems and cryptographic hardware have created a secure post-quantum environment for state electronic information resources.

Keywords: special purpose data transmission networks, cryptographic tools, special purpose complexes, information protection means, cyberspace, post-quantum environment, state electronic information resources.

Корченко Анна Олександрівна, д.т.н., доцент, професор кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.

Корченко Анна Александровна, д.т.н., доцент, профессор кафедры безопасности информационных технологий факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета.

Korchenko Anna, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Technology Security, Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.

Іванченко Євгенія Вікторівна, к.т.н., професор, професор кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.
Иванченко Евгения Викторовна, к.т.н., профессор, профессор кафедры безопасности информационных технологий факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета.
Ivanchenko Yevheniya, Candidate of Technical Sciences, Professor, Professor of the Department of Information Technology Security, Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.

Кошкіна Наталія Василівна, д.т.н., старший науковий співробітник, старший науковий співробітник відділу оптимізації чисельних методів, Інститут кібернетики імені В.М. Глушкова НАН України.
Кошкина Наталья Васильевна, д.т.н., старший научный сотрудник, старший научный сотрудник отдела оптимизации численных методов, Институт кибернетики имени В.М. Глушкова НАН Украины.
Koshkina Natalia, Doctor of Technical Sciences, Senior Researcher, Senior Research Fellow, Department of Optimization of Numerical Methods, Institute of Cybernetics Glushkova NAS of Ukraine.

Кузнецов Олександр Олександрович, д.т.н., професор, професор кафедри безпеки інформаційних систем і технологій факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна, заступник головного конструктора приватного акціонерного товариства «Інститут інформаційних технологій».
Кузнецов Александр Александрович, д.т.н., профессор, профессор кафедры безопасности информационных систем и технологий факультета компьютерных наук Харьковского национального университета имени В. Н. Каразина, Заместитель главного конструктора частного акционерного общества «Институт информационных технологий».
Kuznetsov Oleksandr, Doctor of Technical Sciences, Professor, Professor of the Department of Information Systems Security and Technologies, Faculty of Computer Science, VN Karazin Kharkiv National University, Deputy Chief Designer of the Private Joint-Stock Company "Institute of Information Technologies".

Качко Олена Григорівна, к.т.н., професор, професор кафедри програмної інженерії факультету комп'ютерних наук Харківського національного університету радіоелектроніки, заступник головного конструктора приватного акціонерного товариства «Інститут інформаційних технологій».
Качко Елена Григорьевна, к.т.н., профессор, профессор кафедры программной инженерии факультета компьютерных наук Харьковского национального университета радиоэлектроники, заместитель главного конструктора частного акционерного общества «Институт информационных технологий».
Kachko Olena, Candidate of Technical Sciences, Professor, Professor of the Department of Software Engineering, Faculty of Computer Science, Kharkiv National University of Radio Electronics, Deputy Chief Designer of the Private Joint-Stock Company "Institute of Information Technologies".

Потій Олександр Володимирович, д.т.н., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України.
Потий Александр Владимирович, д.т.н., профессор, заместитель Председателя Государственной службы специальной связи и защиты информации Украины.
Potiy Oleksandr, Doctor of Technical Sciences, Professor Deputy Head of the State Service for Special Communications and Information Protection of Ukraine.

Онопрієнко Віктор Васильович, кт.н., старший науковий співробітник, генеральний директор приватного акціонерного товариства «Інститут інформаційних технологій».
Оноприенко Виктор Васильевич, к.т.н., старший научный сотрудник, генеральный директор частного акционерного общества «Институт информационных технологий».
Onoprienko Viktor, Candidate of Technical Sciences, Senior Researcher General Director of the Private Joint-Stock Company "Institute of Information Technologies".

Бобух Всеволод Анатолійович, к.т.н., начальник відділу апаратних засобів захисту інформації приватного акціонерного товариства «Інститут інформаційних технологій».
Бобух Всеволод Анатольевич, начальник отдела аппаратных средств защиты информации частного акционерного общества «Институт информационных технологий».
Bobukh Vsevolod, Candidate of Technical Sciences, Head of the Department of Information Protection Hardware of the Private Joint-Stock Company "Institute of Information Technologies".

Отримано *22 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*

125 Кібербезпека (1. Управління інформаційною безпекою; 2. Системи та технології кібербезпеки) *– приймаються особи з повною загальною середньою освітою та особи, які здобули освітньо-кваліфікаційний рівень молодшого спеціаліста (на 2-й курс за умови ліквідації академічної заборгованості). Зарахування проводиться за конкурсом – сертифікат УЦОЯО з таких дисциплін: 1) українська мова та література; 2) математика; 3) іноземна мова або фізика.*

та магістратури:

125 Кібербезпека (Адміністративний менеджмент у сфері захисту інформації)

124 Системний аналіз (Консолідована інформація)

Навчальний процес на кафедрі безпеки інформаційних технологій (БІТ) проходить у сучасних спеціалізованих навчальних та навчально-наукових лабораторіях, комп'ютерних класах та полігонах, де студенти отримують ґрунтовні знання з гуманітарних, соціально-економічних, математичних, природничо-наукових та професійних дисциплін. Протягом навчання ***студент оволодіє*** сучасними інформаційними технологіями, що дозволить йому досконало знати конструкцію та принципи функціонування і захисту сучасних комп'ютерів та операційних систем, організовувати захищений електронний документообіг, адмініструвати та захищати комп'ютерні мережі, проектувати комплексні системи захисту інформації та системи управління інформаційною безпекою тощо. ***Випускник кафедри БІТ*** здатний вирішувати завдання теоретичного та практичного характеру, що безпосередньо пов'язані з усіма без винятку аспектами захисту інформації. Випускники займають керівні посади у державних комітетах, службах та міністерствах, авіапідприємствах, банківських та ін. державних і недержавних установах. Крім того, кращі випускники можуть продовжити навчання в аспірантурі (докторантурі). Іногородні студенти на час навчання ***забезпечуються гуртожитками.***

Викладачі кафедри БІТ є досвідченими фахівцями у галузі інформаційної та авіаційної безпеки, вони набували досвіду в престижних навчальних закладах Європи та світу. Більшість викладачів є дійсними членами Міжнародної організації електротехніки та електроніки (IEEE), а їх висока кваліфікація підтверджена професійними сертифікатами та дипломами. Викладачі кафедри активно займаються науковою діяльністю і залучають студентів зокрема до участі у наукових конгресах, симпозіумах, конференціях та семінарах. З метою обміну досвідом та поглиблення освітнього рівня фахівців, ***кафедра тісно співпрацює*** з *СБУ, Державною службою спеціального зв'язку та захисту інформації України, Академією СБУ, Одеською національною академією зв'язку ім. О.С. Попова, Харківським національним університетом радіоелектроніки, Національним університетом «Львівська політехніка», Інститутом фізики НАН України, Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Інститутом кібернетики ім. В.М. Глушкова НАН України, Державним науково-дослідним інститутом спеціального зв'язку та захисту інформації, Вірменським державним інженерним університетом (м. Єреван, Вірменія), Казахським національним технічним університетом ім. К.І. Сатпаєва (м. Алмати, Казахстан), Центрально-азіатським університетом (м. Алмати, Казахстан), Університетом у Бельсько-Бялій (Польща), Державною вищою технічною школою у Новому Сончі (Польща), компаніями Аххоп Soft, SI BIS, D-Link, Сайфер, Криптон, Арт-мастер, Нові пошукові технології та ін*

НАУКОВЕ ВИДАННЯ

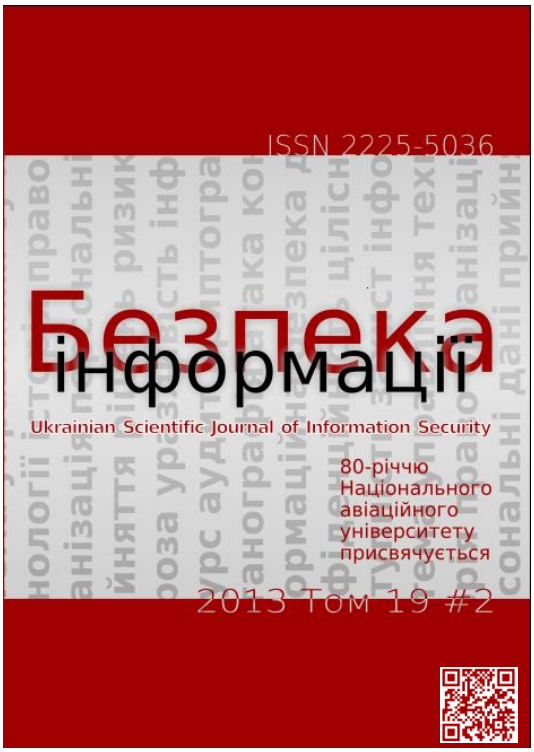
БЕЗПЕКА ІНФОРМАЦІЇ

Ukrainian Scientific Journal of Information Security

Міжнародним центром ISSN (Париж, Франція) журналу присвоєно міжнародний стандартний номер для періодичних видань (International Standard Serial Number):
ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
У міжнародний Реєстр ISSN журнал занесено під такими назвами:
Ключова назва (Key title): ***Bezpeka ìnformacìì***
Скорочена ключова назва (Abbreviated key title): ***Bezpeka ìnf.***

У авторській редакції
Комп'ютерне макетування: Анна Володимирівна ЩЕРБИНА
Дизайн обкладинки та логотипу: Кирило Петрович АНУФРІЄНКО

Підписано до друку 29.04.2021 р. Формат 60 × 84/8 Офс. друк Ум. друк. арк. 5,0. Обл. вид. арк. 5,4. Наклад 300 прим. Замовлення №_____ Віддруковано у типографії «Наш формат» 00105, м. Київ, пр. Миру 7.



Передплатний індекс та вартість річної підписки:

68979
581.61 грн./рік
(виходить 3 рази на рік – у квітні, серпні та грудні)

89539
775.45 грн./рік
(виходить 4 рази на рік – у березні, червні, вересні та грудні)