«Информатика, кибернетика и вычислительная техника»

Научная статья
УДК 004.054.53
DOI: 10.17072/1993-0550-2023-1-63-69

# Опыт создания макета критической инфраструктуры организации

**Сергей Николаевич Горячев[1], Вадим Валерьевич Михалев[2], Николай Сергеевич Кобяков[3], Владислав Николаевич Русских[4]**
[1, 2, 3, 4] Пермский военный институт войск национальной гвардии Российской Федерации, Пермь, Россия
[1]sergory@mail.ru, https://orcid.org/0000-0002-6994-8559
[2]michalev.vd992@yandex.ru, https://orcid.org/0000-0002-0230-2874
[3]kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879
[4] vladislav.grom628@yandex.ru, https://orcid.org/0000-0002-0530-3356

**Аннотация**. В статье описывается разработанный авторами лабораторный комплекс киберполигона для обучения навыкам отражения компьютерных атак специалистами информационных технологий. Основа лабораторного комплекса опирается на модель критической инфраструктуры объекта Росгвардии. Использование данного комплекса повлияет на интенсификацию и активизацию обучения в вопросах информационной безопасности за счет моделирования компьютерных атак и отработки реакций на них, а также визуализации данных процессов.

**Ключевые слова:** *лабораторный комплекс; компьютерная атака; защита от компьютерных атак; киберполигон; критическая информационная инфраструктура; информационная безопасность*

**Для цитирования:** *Горячев С. Н., Михалев В. В., Кобяков Н. С., Русских В. Н.* Опыт создания макета критической инфраструктуры организации // Вестник Пермского университета. Математика. Механика. Информатика. 2023. № 1(60). С. 63–69. DOI: 10.17072/1993-0550-2023-1-63-69.

*Статья поступила в редакцию 29.11.2022; одобрена после рецензирования 27.01.2023; принята к публикации 15.03.2023.*

«Computer Science, Cybernetics and Computing»

Research article

# Experience in an Organization Critical Infrastructure Layout Creating

**Sergey N. Goryachev[1], Vadim V. Mikhalev [2], Nikolay S. Kobyakov[3], Vladislav N. Russkikh[4]**
[1, 2, 3, 4] Perm Military Institute of National Guard Troops, Perm, Russia
[1]sergory@mail.ru, https://orcid.org/0000-0002-6994-8559
[2]michalev.vd992@yandex.ru, https://orcid.org/0000-0002-0230-2874
[3]kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879
[4] vladislav.grom628@yandex.ru, https://orcid.org/0000-0002-0530-3356

**Abstract**. The article describes developed by the authors the cyberpolygon laboratory complex. It uses for teaching repelling computer attacks skills by information technology specialists. The laboratory complex basis is the critical infrastructure of the facility Rosguard model. The complex using will affect the training intensification and activation by information security issues. It allow to simulate computer attacks, work out reactions to them and visualize of these processes.

**Keywords:** *laboratory complex; computer attack; protection against computer attacks; cyberpolygon, critical information infrastructure; information security*

**For citation:** *Goryachev S. N., Mikhalev V. V., Kobyakov N. S., Russkikh V. N.* Experience in an Organization Critical Infrastructure Layout Creating. Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2023;1(60): 63-69. (In Russ.). DOI: 10.17072/1993-0550-2023-1-63-69.

*The article was submitted 29.11.2022; approved after reviewing 27.01.2023; accepted for publication 15.03.2023.*

## Введение

С начала спецоперации на нашу страну направлена беспрецедентная волна атак. Они идут в трех плоскостях: массовые DDoS-атаки, нацеленные на вывод из строя социально-значимых государственных информационных ресурсов, атаки на средства массовой информации и таргетированные атаки на критическую информационную инфраструктуру [2].

На территории Украины против Российской Федерации в информационном пространстве действует огромная по своим масштабам киберкампания, ежедневно государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы России в среднем фиксирует более 200 комплексных компьютерных атак. При этом специалистам стало известно, что атаки, которые проводятся из разных стран, четко скоординированы [3]. Создание лабораторного комплекса киберполигона позволит повысить эффективность и качество обучения специалистов информационных технологий в вопросах защиты информации в компьютерных сетях. Большое количество функциональных возможностей, которые присутствуют в данном учебном комплексе, способствуют простоте уяснения информации в период прохождения занятия, а также наглядности результатов проверки их знаний, проверяемых тестами по работе программ [4].

## 1. Понятие "киберполигон"

Киберполигон – инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них [1].

Практика симуляции атак поможет выявлять слабые места в ИТ-инфраструктуре, не прибегая к деструктивным тестам собственных ресурсов [5].

Какая бы модель угроз не использовалась, Киберполигон поможет масштабировать ландшафт угроз за счет автоматизации, предоставляя возможность выполнять быстрее и больше симуляций, чем с помощью ручных методов и привлечением пентестеров [5].

В отличие от теоретических занятий и тренингов, в процессе эксплуатации Киберполигона специалисты глубоко поймут методы, используемые передовыми хакерскими группами и научатся им противостоять на практике. Производится реальная демонстрация и обучение противостоянию атакам с самого начала: проникновение в периметр извне, затем продвижение по сети и повышение привилегий, получение контроля над сетью и эксфильтрация данных за контролируемый сетевой периметр [5].

В процессе киберучений будет выявлено, какие ошибки были допущены специалистами в процессе их проведения. Таким образом, специалисты проходят обучение на киберполигоне и получают полезный опыт, без ущерба безопасности, вследствие чего становятся способны противостоять реальным угрозам информационной безопасности [5].

### 1.1. Цели разработки

Разработка лабораторного комплекса киберполигона, с помощью которого специалисты информационных технологий смогут совершенствовать свои знания [4], умения и навыки практической отработки противодействия компьютерным атакам.

Повышение понимания информационной безопасности.

### 1.2. Существующие проблемы

Исследования показали, что большинство организаций не готовы к кибератакам. Примерное время выявления инцидента составляет около 80–100 дней, что более чем достаточно для закрепления и эксфильтрации необходимых данных. К сожалению, у специалистов недостаточно навыков для оперативного реагирования, не проводится регулярных тренировок на противодей-

ствие атакам, отражающим актуальные тенденции в области кибербезопасности [5]. Чаще всего отсутствие полноценного и корректно настроенного мониторинга приводит к невозможности расследования инцидента.

С другой стороны, мониторинг может быть "забит" шумом, что приводит к невозможности быстрого и корректного реагирования [5]. Студенты в процессе обучения не получают ту долю практики, которую могут извлечь из реальных инцидентов [5].

Специалисты извлекают опыт только из реальных инцидентов, которых может быть не так много [5]. По причине отсутствия опыта, успешная атака может быть замечена слишком поздно [5].

### 1.3. Требования к киберполигону

К киберполигону предъявили следующие требования:

1. Созданный сегмент, должен имитировать процессы и сценарии кибератак, свойственных для объекта Росгвардии.

2. Должен быть ориентирован как на специалистов информационной безопасности, так и специалистов информационных технологий.

3. Перечень системного и прикладного программного обеспечения должен состоять из отечественного и иностранного производства.

4. Возможность проведения анализа по произвольному количеству идущих подряд периодов компьютерных атак и ведения с нарастающим итогом.

5. Возможность настройки как исходной инфраструктуры (в том числе сложной), так и возможность пользователю самостоятельно создавать такие описания.

6. Поддержка параметра времени, то есть возможность задавать значения различных параметров с привязкой ко времени.

7. Возможность проведения сравнительного анализа нескольких инфраструктур.

8. Наличие набора готовых сценариев компьютерных атак и сценариев противодействия им.

### 1.4. Значение киберполигона в образовательной деятельности

В ходе тренировок участники совершенствуют навыки оценки защищенности инфраструктуры, отражают смоделированные компьютерные атаки, проводят расследование инцидентов информационной безопасности [6].

Руководитель занятия заранее подготавливает сценарий нештатных ситуаций. На лабораторном комплексе возможно использование как типовых сценариев атак, так и модифицированных под нужды конкретного объекта [6].

Повышение защищенности означает постоянное сокращение поверхности атаки и минимизации времени реагирования. Новые приложения, серверы и IT-устройства появляются и устанавливаются каждый день, создавая новые возможности для хакеров. К тому же новые эксплойты могут свести защиту защищенных систем на нет [5].

Учебные тренировки будут максимально приближены к реальным боевым условиям. Лица, прошедшие обучение, приобретут новые профессиональные навыки и в дальнейшем смогут эффективно реагировать на угрозы информационной безопасности [6].

Но навыки смогут получить конечно, только там, где открыты специальные классы с доступом к инфраструктуре киберполигона, поэтому и требуется создать его в институте.

Когда мы говорим о преимуществах цифровой экономики, важно учитывать те риски, которые она несет. Прежде всего, речь идет об угрозах, позволяющих киберпреступникам похитить ценную информацию, нарушить функционирование критической информационной инфраструктуры и повлиять на привычную жизнь большого количества людей [6].

Так, современные киберпреступники способны получить контроль над автоматизированными системами управления технологическими процессами (АСУ ТП) и парализовать производство, получить доступ к банковским системам и похитить деньги клиентов. В зависимости от сферы это может привести к значительным финансовым потерям отдельной компании и даже риску техногенной катастрофы, если речь идет о промышленных предприятиях [6].

## 2. Разработка киберполигона

Сравнительный анализ имеющихся на рынке готовых платформ киберполигонов показал, что на данный момент не существует платформы, удовлетворяющей всем перечисленным требованиям и учитывающей специфику автоматизированной системы специального назначения, поэтому было принято решение создать лабораторный комплекс киберполигона самостоятельно.

Лабораторный комплекс киберполигона был спроектирован и частично реализован

инициативной группой на кафедре вычислительных машин, комплексов, систем и сетей Пермского военного института ВНГ РФ.

Рассмотрим его состав, структуру и функции:

При создании лабораторного комплекса киберполигона разработаны: сегмент для ИТ-инфраструктуры ("ИТ-сегмент"); сегмент для инфраструктуры жизнеобеспечения ("сегмент жизнеобеспечения"); центр управления комплексом ("Управляющий сегмент"). Структурная схема предоставлена на рис. 1.

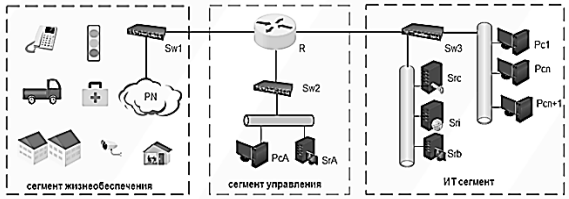


**Рис. 1.** *Структурная схема лабораторного комплекса киберполигона*

"ИТ-сегмент" состоит из серверной части (Src, Sn, Srb) и рабочих мест обучаемых (Pc1, Pcn … Pcn+1). К серверной части предъявляются повышенные требования к аппаратной части, так как на ней установлены среда виртуализации с виртуальными серверами информационных систем, имеющих уязвимости, ошибки конфигурирования и настройки. Рекомендуется применять компьютер с процессором Intel Core i7 или эквивалентным, объемом оперативной памяти 32 Гб, накопитель типа SSD объемом от 500 Гб. Он предназначен для хранения данных объектов сегмента жизнеобеспечения.

В качестве автоматизированных рабочих мест обучающихся применяются рабочие станции с свободно распространяемым дистрибутивом Kali Linux. Kali Linux создан на основе операционной системы Debian с открытым исходным кодом, предназначен для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности, компьютерная криминалистика и обратный инжиниринг [7]. Рекомендуется применять компьютеры с процессором Intel Core i3 или эквивалентным, объемом оперативной памяти 2 Гб, накопители типа НЖМД или SSD объемом от 100 Гб.

Центр управления комплексом ("Управляющий сегмент") предназначен для связи между сегментами и настройки их взаимодействия, определения работоспособности узлов, изменения настроек работы и расширения сети методом добавления новых узлов.

Обеспечение информационной безопасности на критически важных объектах, обуславливается современными условиями деятельности с применением информационной и телекоммуникационной инфраструктуры, а также большим количеством потенциальных угроз как случайного, так и преднамеренного характера. В "сегменте жизнеобеспечения" находятся значимые объекты жизнеобеспечения оборудование которых взаимодействуют как через промышленные протоколы управления, так и сетевые протоколы передачи данных. К таким объектам отнесены жилые здания, склады, объекты энергетики, тепло-, водоснабжения, транспортной сферы, системы контроля управления доступом, видеонаблюдения и другие.

### 2.1. 3D-модель киберполигона

Реализован участок киберполигона ПВИ ВНГ РФ в виде макета в составе:

1. Учебный корпус факультета связи;
2. Казарма № 6;
3. Классы артиллерийского вооружения;
4. Общежитие курсов повышения квалификации;
5. КПП № 2.

3D-модель представлена на рис. 2.

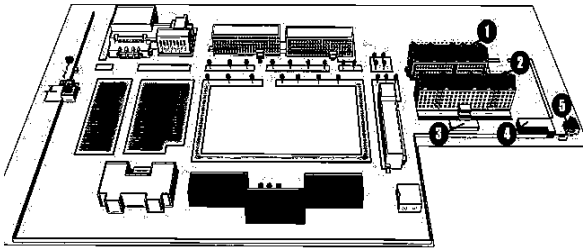

**Рис. 2.** *Структурная схема лабораторного комплекса киберполигона*

На рис. 3 представлена воссозданная модель КПП № 2.

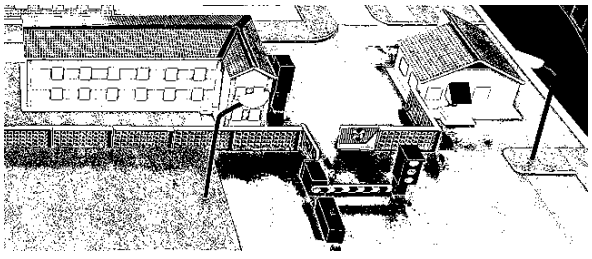

**Рис. 3.** *Модель КПП № 2*

На данном участке макета развернута действующая инфраструктура:

1. Автоматизация пропускного режима транспортных средств на территорию института (на базе контроллера Arduino Nano).

В целях экономии денежных ресурсов используется контроллер Arduino Nano. Управление осуществляется через программный код программы управления, представлен в табл. 1, 2, 3.

**Таблица 1.** *Программный код управления светофорами*

| *Светофор 1* | *Светофор 2* |
|---|---|
| #define PIN_LIGHT_RED1 13<br>#define PIN_LIGHT_YELLOW1 12<br>#define PIN_LIGHT_GREEN1 11 | #define PIN_LIGHT_RED2 A3<br>#define PIN_LIGHT_YELLOW2 A4<br>#define PIN_LIGHT_GREEN2 A5 |

**Таблица 2.** *Программный код управления датчиками расстояния*

| *Датчик расстояния 1* | *Датчик расстояния 2* |
|---|---|
| #define PIN_ECHO1 5<br>#define PIN_TRIG1 6<br>#define PIN_SENSOR1 9 | #define PIN_ECHO2 7<br>#define PIN_TRIG2 8<br>#define PIN_SENSOR2 10 |

**Таблица 3.** *Программный код управления сервоприводами*

| *Сервоприводы* |
|---|
| #define PIN_SERV1 2<br>#define PIN_SERV2 3<br>#define PIN_SERV3 4 |

2. Управление внешним освещением и освещением в зданиях с использованием АРМ (контроллер Omron CP1L).

Освещение организовано по методу принципиальной электрической схемы светодиодов. Схема предоставлена на рис. 4.

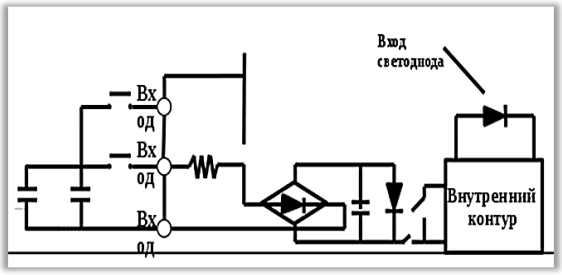


**Рис. 4.** *Принципиальная электрическая схема светодиодов*

Управление освещением осуществляется с помощью специального программного обеспечения. Фрагмент программы представлен на рис. 5.

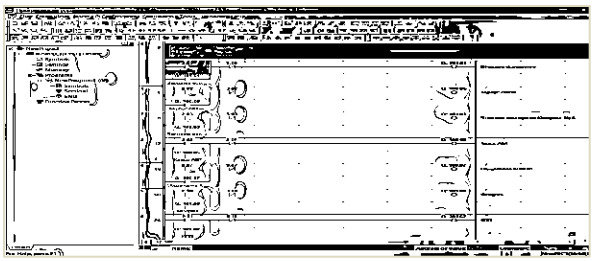

**Рис. 5.** *Фрагмент программы управления освещением*

### 2.2. Экономическая составляющая с учетом развития киберполигона

В табл. 4 предоставлена экономическая составляющая макета критической инфраструктуры, разработанного в ПВИ ВНГ РФ с учетом его дальнейшего развития.

### 2.3. Перспективы дальнейшего развития

В рамках масштабирования киберполигона планируется создать следующие объекты:

1) КПП № 1;
2) физкультурно-оздоровительный комплекс;
3) учебный корпус № 1;
4) учебный корпус № 2;
5) казарма факультета тыла;
6) курсантская столовая;
7) казарма № 3;
8) казарма № 2;
9) казарма № 1;
10) банно-прачечное отделение;
11) деревья в масштабе 1:100;
12) фонарные столбы в масштабе 1:100;
13) ворота на КПП № 1;
14) установка светофора и шлагбаума на КПП № 1 в масштабе 1:100;
15) замена самодельных светофоров и шлагбаума на КПП № 2 на заводские модели в масштабе 1:100.

Перспективное развитие макета киберполигона предоставлено на рис. 6.

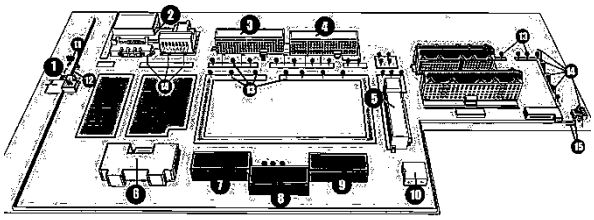

**Рис. 6.** *Перспективное развитие макета киберполигона ПВИ ВНГ РФ*

**Таблица 4.** *Экономическая составляющая макета критической инфраструктуры, разработанного в ПВИ ВНГ РФ с учетом его дальнейшего развития*

| N *п/п* | *Наименование* | *кол-во* | *цена, шт.* | *цена, всего* |
|---|---|---|---|---|
| 1. | Arduin Nano | 3 | 800 | 2400 |
| 2. | Arduin Uno R3 smd | 1 | 770 | 770 |
| 3. | Светодиодная лента 12В 5 м | 3 | 1000 | 3000 |
| 4. | Светодиоды (красные, зелёные, жёлтые, белые) | 100 | 20 | 2000 |
| 5. | Блок питания 12В (35Вт) | 3 | 1000 | 3000 |
| 6. | Датчик движения | 5 | 340 | 1700 |
| 7. | Сервопривод S690 | 5 | 400 | 2000 |
| 8. | Эхолокатор HC SR04 | 2 | 300 | 600 |
| 9. | Датчик расстояния (положения) | 5 | 400 | 2000 |
| 10. | Интернет модуль W5100 для Arduino Uno | 1 | 750 | 750 |
| 11. | Макет дерева в масштабе 1:100 | 40 | 125 | 5000 |
| 12. | Макет фонарного столба в масштабе 1:100 | 30 | 50 | 1500 |
| 13. | Макет светофора в масштабе 1:100 | 5 | 400 | 2000 |
| 14. | Материал для имитации газона 50х100 | 2 | 1130 | 2260 |
| 15. | Реле 12В | 10 | 50 | 500 |
| 16. | ЖК дисплей для Arduino | 1 | 400 | 400 |
| 17. | Модуль NRF24L01 | 1 | 270 | 270 |
| 18. | Вспененный ПВХ 5 мм (2000х1000) (основания) | 2 | 3000 | 6000 |
| 19. | Вспененный ПВХ 3 мм (2000х1000) (здания) | 3 | 3000 | 9000 |
| 20. | Ламинат А3 125 мкн | 1 | 3000 | 3000 |
| 21. | Фанера | 1 | 3000 | 3000 |
| 22. | Деревянный брусок размером 2000х40х40 | 2 | 500 | 1000 |
| 23. | Ножки для стола | 4 | 600 | 2400 |
| 24. | Уголки металлические 40х40 | 4 | 250 | 1000 |
| 25. | Расходные материалы (клей, хомуты, саморезы) | | | 3000 |
| | | | ИТОГО: | 58550 |

## Заключение

Таким образом, киберполигон поможет курсантам и специалистам информационных технологий ВНГ РФ практическим методом отработать порядок действий при возникновении компьютерных инцидентов. Существенно увеличится уровень подготовки специалистов в области информационной безопасности в ВНГ РФ, а значит и уровень информационной безопасности войск в целом.

Дальнейшим направлением развития лабораторного комплекса в ПВИ ВНГ РФ является разработка тестовых виртуальных машин с установленными на них различными типами геоинформационных систем или систем сбора пространственно-временных данных.

## Список источников

1. *Постановление* Правительства РФ от 12 октября 2019 г. № 1320 "Об утверждении Правил предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности" (с изменениями и дополнениями).
2. *Интервью* с экспертом: "Киберучения на ПМЭФ-2022: тренировка навыков и организация взаимодействия". URL: https://safe-surf.ru/specialists/article/5300/680631/?ysclid=l9jo7z3rvd877405325 (дата обращения: 20.10.2022).
3. *Стало* известно о беспрецедентных кибератаках на Россию. URL: https://lenta.ru/news/2022/07/06/cybercampania (дата обращения: 20.10.2022).
4. *Концепция* создания киберполигона для обучения специалистов в области информационной безопасности / *Хорзова И.С.* Информационные технологии в деятельности органов внутренних дел. URL: https://elibrary.ru/item/asp?id=45760221 (дата обращения: 20.10.2022).

5. *Киберполигон* – мультифункциональный комплекс для проведения киберучений. URL: https://habr.com/ru/post/80586 (дата обращения: 20.10.2022).
6. *В России* создается Национальный киберполигон. О самом масштабном проекте в сфере информационной безопасности страны. URL: https://ib-bank.ru/bisjournal/post/1587 (дата обращения: 20.10.2022).
7. *Kali* Linux на основе операционной системы Debian. URL: http://www/ruslinux.net/lib.php?name=%2FMyLDP%2Findex.html (дата обращения: 20.10.2022).

## References

1. *Postanovlenie* Pravitel'stva RF ot 12 oktyabrya 2019 g. N 1320 "Ob utverzhdenii Pravil predostavleniya subsidij iz fe-deral'nogo byudzheta na vvedenie v eks-pluataciyu i obespechenie funkcioniro-vaniya kiberpoligona dlya obucheniya i tre-nirovki specialistov i ekspertov razno-go profilya, rukovoditelej v oblasti in-formacionnoj bezopasnosti i in-forma-cionnyh tekhnologij sovremennym prak-tikam obespecheniya bezopasnosti" (s iz-meneniyami i dopolneniyami). (In Russ.).
2. *Interv'yu* s ekspertom: "Kiberucheniya na PMEF-2022: trenirovka navykov i organizaciya vzaimodejstviya". URL: https://safe-surf.ru/specialists/article/5300/680631/?ysclid=l9jo7z3rvd877405325 (accessed: 20.10.2022).
3. *Stalo* izvestno o besprecedentnyh kiberatakah na Rossiyu. URL: https://lenta.ru/news/2022/07/06/cybercampania (accessed: 20.10.2022).
4. *The concept* of creating a cyberpolygon for training specialists in the field of information security / Horzova I.S. Information technologies in the activities of internal affairs bodies. URL: https://elibrary.ru/item/asp?id=45760221 (accessed: 20.10.2022).
5. *Kiberpoligon* – mul'tifunkcional'nyj kompleks dlya provedeniya kiberuchenij. URL: https://habr.com/ru/post/80586 (accessed: 20.10.2022).
6. *V Rossii* sozdayotsya Nacional'nyj kiber-poligon. O samom masshtabnom proekte v sfere informacionnoj bezopasnosti strany. https://ib-bank.ru/bisjournal/post/1587 (accessed: 20.10.2022).
7. *Kali* Linux based on the Debian operating system. URL: http://www/ruslinux.net/lib.php?name=%2FMyLDP%2Findex.html (accessed: 20.10.2022).

**Информация об авторах:**

*С. Н. Горячев* – начальник кафедры вычислительных машин, комплексов, систем и сетей факультета связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д.1), AuthorID 993073;

*В. В. Михалев* – старший преподаватель кафедры вычислительных машин, комплексов, систем и сетей факультета связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д.1);

*Н. С. Кобяков* – начальник учебной лаборатории технической защиты информации кафедры вычислительных машин, комплексов, систем и сетей факультета связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д.1), AuthorID 1126165;

*В. Н. Русских* – курсант факультета связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д.1).

**Information about the authors:**

*S. N. Goryachev* – Head of the Department of Computers, Complexes, Systems and Networks, Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log Street, Perm, Russia, 614112), AuthorID 1126165;

*V. V. Mikhalev* – Senior teacher of the Department of Computers, Complexes, Systems and Networks, Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log Street, Perm, Russia, 614112);

*N. S. Kobyakov* – Head of the Educational Laboratory of Technical Information Protection, Department of Computers, Complexes, Systems and Networks, Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log Street, Perm, Russia, 614112), AuthorID 1126165

*V. N. Russkikh* – Cadet of the Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log Street, Perm, Russia, 614112).