ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2022, том 3, № 4, с. 401–406

ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

УДК 004.056

РАЗРАБОТКА И ВНЕДРЕНИЕ КИБЕРПОЛИГОНА В ПРОЦЕСС ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

© 2022 г. В. В. Баранов[1,*], А. П. Корчагина[1]

[1] *Южно-Российский государственный политехнический университет им. М.И. Платова (Новочеркасский политехнический институт), Новочеркасск, Россия*

*****E-mail: baranov.vv.2015@yandex.ru*

Поступила в редакцию 15.03.2022 г.
После доработки 20.03.2022 г.
Принята к публикации 20.03.2022 г.

Обучение специалистов в области информационной безопасности невозможно без отработки практических навыков. В рамках освоения учебных дисциплин возможны разработка и применение киберполигона. Эта задача подразумевает множество проблем. В работе рассмотрены основные из них, а также возможные пути решения.

DOI: 10.56304/S2782375X22040027

ВВЕДЕНИЕ

При обучении студентов по программам специалитета и магистратуры по направлению 10.00.00 “Информационная безопасность” в рамках освоения учебных дисциплин необходимо, чтобы студенты научились работать с современными средствами мониторинга событий информационной безопасности и защиты в реальных условиях реализации атак на информационную систему предприятия.

Одним из эффективных решений по обеспечению получения навыков практических действий в сфере обеспечения кибербезопасности является внедрение в учебный процесс технологии киберполигона.

Киберполигон – это мультифункциональный программно-аппаратный комплекс для проведения киберучений путем моделирования компьютерных атак и отработки реакций на них [1].

В настоящее время на рынке представлены различные программно-технические решения в данной области. Наиболее популярными из них являются: “Ampire” от компании “Перспективный мониторинг” и “Национальный киберполигон” от компании “Ростелеком-Солар”.

Внедрение любого из указанных комплексов в учебный процесс значительно упростит восприятие теоретической информации в области кибербезопасности. Обучаемые смогут получить навыки по отработке выявления компьютерных атак и расследований инцидентов информационной безопасности, оценке защищенности элементов информационных систем, организации взаимодействия между группами специалистов, закрытии инцидента и ликвидации его последствий.

Отметим, что киберполигон является дорогостоящим полноценным комплексом. С финансовой точки зрения внедрение в учебный процесс такого решения будет обладать длительным сроком окупаемости. В связи с этим возникает проблема поиска альтернативных решений. Одним из возможных направлений может стать разработка своими силами платформы киберполигона меньшего масштаба.

Процесс проектирования и разработки подразумевает работу нескольких групп специалистов и заключает в себе решение разнообразных технических, методических, организационных и иных проблем.

МЕТОДЫ

Использование киберполигона в учебном процессе является актуальным и эффективным решением и должно осуществляться путем решения следующих задач:

– разработка и анализ модели будущего киберполигона и оптимизация его структуры;

– создание сопроводительной документации, включающей в себя варианты сценариев кибератак, методические указания для студентов и преподавателей, руководство по эксплуатации и иные документы, необходимые для успешного функционирования киберполигона;

– разработка веб-интерфейсов, необходимых для реализации достаточной степени визуализации сценариев обстановки, обеспечивающих ин-

туитивное понимание стоящих задач и правил использования комплекса;

– возможность анализа нескольких вариаций отчетности по результатам обучения как отдельных студентов, так и группы в целом;

– разработка системы оценивания действий обучаемых при проведении киберучений.

Содержание технического задания на разработку киберполигона может варьироваться в зависимости от требуемого функционала. При этом должны быть сформулированы общие принципы.

1. Разработка киберполигона должна проводиться на базе отечественных операционных систем и прикладного программного обеспечения (**ПО**).

2. Сопроводительная документация должна быть подробной, конкретизированной и хорошо структурированной. Это позволит снизить время поиска необходимой информации, а также улучшит работу с ней.

3. Все разрабатываемые веб-интерфейсы должны обладать высокой степенью визуализации и информативности, а используемые символы – понятны интуитивно. В этом случае целесообразно применить распространенные обозначения и способы оценивания.

4. Веб-интерфейс руководителя тренировки должен отражать отчеты с разной степенью детализации. Это позволит преподавателю оценивать не только результат действий группы студентов, но и использовать индивидуальный подход в зависимости от того, как проявил себя каждый обучаемый.

Для удобства эксплуатации архитектуру киберполигона целесообразно реализовать с помощью виртуальных машин. В зависимости от выбранной задачи проводится их запуск и формируется сетевое окружение, включающее в себя различные устройства, в целом имитирующие информационную инфраструктуру предприятия.

На основе сценария, заданного преподавателем, происходит генерация логинов, паролей и IP-адресов для каждой виртуальной машины. Действия разворачиваются в виртуальной среде. Это позволяет не ограничивать свободу действий обучаемых, так как обеспечивает защиту программно-аппаратной части от деструктивных воздействий.

Сценарий проведения занятий может быть структурирован в зависимости от уровня подготовленности группы, ограничений по времени, целей и задач тренировки. Поставленные задачи могут заключаться в выполнении типовых сценариев. Например, защита от атаки на файловый сервер или сервер баз данных, защита центра обработки данных.

На первом этапе киберучений для ознакомления с исходными данными обучаемым предоставляются методические материалы на бумажном носителе либо в электронном виде. Примером исходных данных могут быть структурная схема сети, описание деятельности отдельных структурных подразделений, значимость информации, циркулирующей между ними, а также местоположение критически значимых узлов сети.

При условии достаточности ресурсов желательно разработать несколько вариантов развития событий. Это позволит организовать отработку более широкого спектра навыков.

Для установления равновесия в области ресурсов (как технических, так и человеческих) рациональным решением является упрощение структуры сети при увеличении разнообразия сценариев и, наоборот, увеличение структуры сети при условии уменьшения количества сценариев. В целом условия равновесия и целесообразности устанавливаются исключительно возможностями разработчиков [2].

Структура киберполигона представлена на рис. 1. В его состав включены указанные ниже элементы.

Отметим, что в рамках реализации развертывания киберполигона необходимо предусмотреть следующие роли.

Руководитель тренировки (преподаватель). Имеет автоматизированное рабочее место АРМ, веб-интерфейс которого обеспечивает формирование заданий для проведения тренировки и контроль за действиями обучаемых. Руководителю тренировки предоставляются полномочия администрирования сценариев и процессов. Он осуществляет контроль за действиями группы обучаемых, проводит подготовку рабочей среды для киберучений, устанавливает временные рамки, формирует сценарии, состав подгрупп обучаемых и анализирует их действия.

Группа атакующих. Полномочия группы заключаются в возможности нанесения различных кибератак на информационную инфраструктуру виртуального предприятия. Веб-интерфейс автоматизированного рабочего места группы проведения кибератак предназначен для реализации сценариев кибератак на сеть предприятия. Это позволяет получить практические навыки по проведению пентестов и выявлению слабых мест, уязвимостей защищаемых активов, а также проиллюстрирует базовые задачи, ставящиеся перед “белым” хакером.

Группа защищающихся. По усмотрению руководителя тренировки данная группа может быть разделена или структурирована. Ее обязательными функциями должны быть эксплуатация информационных систем, мониторинг и выявление деструктивных воздействий на информационную

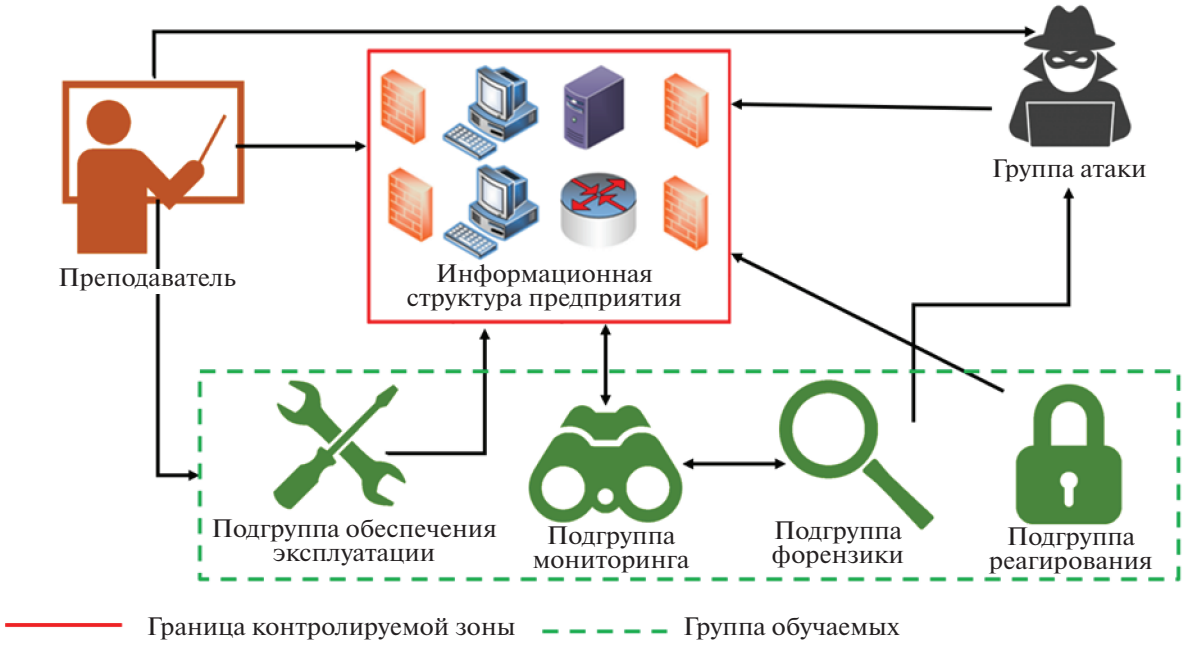

Рис. 1. Структурная схема взаимодействия элементов киберполигона.

инфраструктуру предприятия, фиксация и определение атрибутов инцидента, а также реализация ответных действий по защите активов, закрытие инцидента и ликвидация его последствий.

Исходя из этого в составе данной группы выделен ряд структурных подразделений, выполняющих указанные выше функции.

Подгруппа обеспечения эксплуатации (**ПгОЭ**). Имеет в своем распоряжении АРМ, веб-интерфейс которого позволяет проводить эксплуатацию и обслуживание информационной инфраструктуры предприятия.

Подгруппа мониторинга (**ПгМ**) с помощью специализированного ПО АРМ ведет мониторинг событий информационной безопасности, отслеживает изменения киберобстановки [3, 4].

Подгруппа реагирования на компьютерные инциденты (**ПгРКИ**) осуществляет действия по обеспечению безопасности информационной инфраструктуры предприятия. С помощью веб-интерфейса АРМ регистрируют инциденты, формируют карточки инцидентов с информацией о выявленной кибератаке, фиксируют основные сведения, которые позволят качественно нейтрализовать действия злоумышленников [5–7].

Подгруппа форензики (**ПгФ**) предназначена для расследования источников выявленных кибератак, причин возникновения инцидентов информационной безопасности, а также поиска нарушителей [8]. Данные действия также осуществляют с помощью веб-интерфейса АРМ.

Такой подход обеспечивает наиболее эффективное использование времени, отведенного на выявление, защиту и расследование компьютерных инцидентов. Для преподавателя разделение группы защищающихся позволит упростить процедуру оценки действий подгрупп в целом и отдельно каждого ее участника.

Для обеспечения функционирования такой структуры необходимо создать виртуальную среду, в которой участники смогут реализовывать и фиксировать последовательность своих действий.

Сценариями предусмотрена возможность проведения следующих видов атак [9–11].

Атака на файловый сервер. При реализации данного вида атаки злоумышленник получает доступ к данным, хранящимся на файловом сервере.

Атака на сервер баз данных (**БД**). В данном случае злоумышленник получает доступ к серверу, на котором хранятся БД предприятия.

DDoS-атака. При реализации злоумышленник отправляет запросы на атакуемый сервер, из-за чего происходит сбой. Сервер перегружается запросами, которые не успевает обрабатывать, и прекращает свою работу.

IP-спуффинг. Вид атаки, заключающийся в использовании чужого IP-адреса источника с целью обмана системы безопасности.

Атака “человек посередине”. Особенность атаки заключается в том, что злоумышленник “пропускает” веб-трафик атакуемого через свое устройство. Это позволяет видеть всю информа-

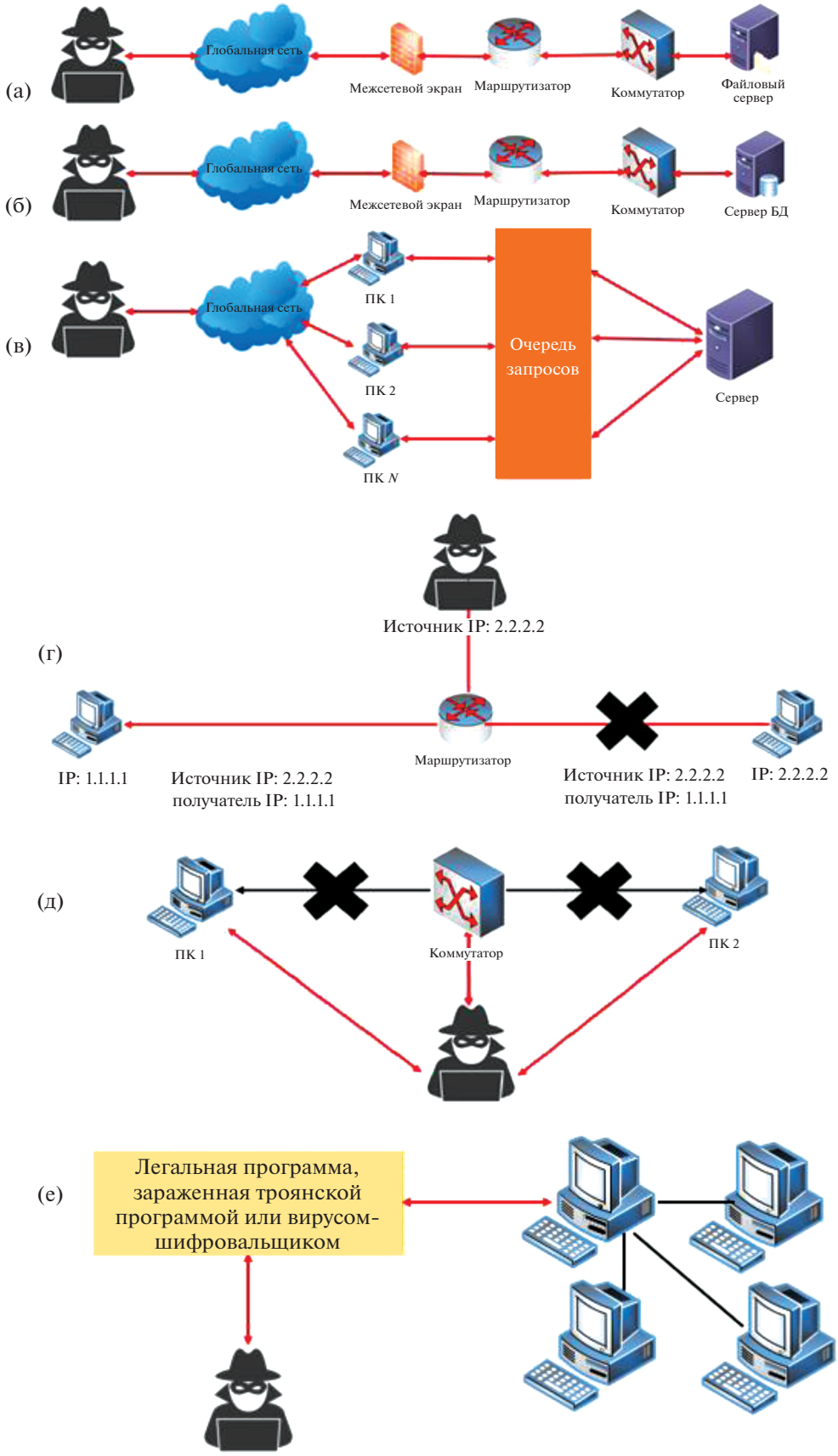

Рис. 2. Структура атак: а – атака на файловый сервер, б – атака на сервер БД, в – DDoS-атака, г – IP-спуффинг, д – атака “человек посередине”, е – атака троянской программы и вируса-шифровальщика.

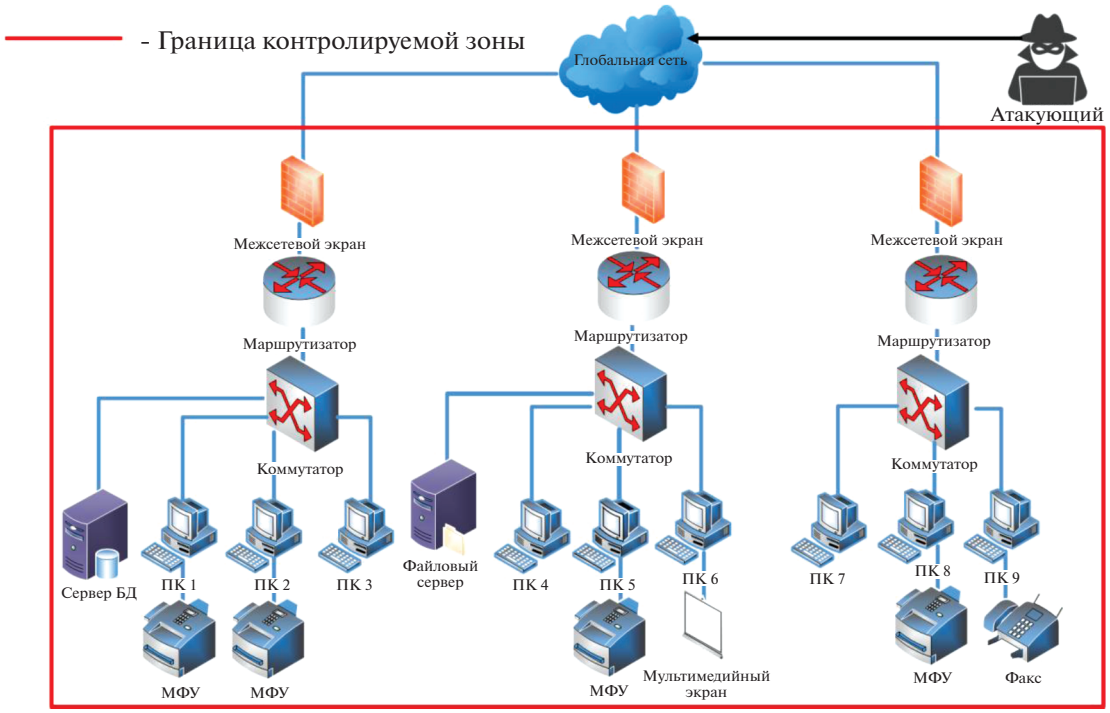

Рис. 3. Вариант построения структуры защищаемой сети.

цию, поступающую на легальное устройство жертвы [9].

Применение троянской программы или вирусов-шифровальщиков. При реализации этой атаки под видом легальной программы в компьютерную сеть предприятия проникает вирус. С его помощью злоумышленник получает доступ к информации, хранящейся на зараженном компьютере, или блокирует компьютер.

Структура проведения данных видов кибератак представлена на рис. 2.

Специализированное ПО киберполигона дает возможность модификации и наращивания сценариев атак и элементов информационной инфраструктуры предприятия.

Для упрощения протоколирования событий информационной безопасности в виртуальной среде оптимальным решением является включение в состав киберполигона SIEM-систем. На рынке представлены разнообразные готовые решения, которые могут быть интегрированы. Одним из наиболее популярных среди них является “KOMRAD Enterprise SIEM” от компании “Эшелон”, который включен с состав киберполигона.

Для применения мер защиты необходимо видеть структуру сети и список выявленных вторжений. Это позволит принять решение по применению целесообразных мер и определить намерения злоумышленников, по возможности предпринять шаги по опережению ситуации.

Разработанный вариант структуры защищаемой сети представлен на рис. 3.

Реализация разнотипных интерфейсов с узкоспециализированным функционалом даст возможность формирования не только практических навыков по атаке на компьютерную сеть и ее защите, но и умению анализировать ситуацию, взаимодействовать с другими специалистами-участниками. Иными словами, в процессе занятия будут сформированы как компетенции, предусмотренные учебными планами, так и улучшены или заложены для дальнейшего развития такие личностные навыки, как умение эффективно взаимодействовать с другими участниками процессов, навыки управленческой деятельности, анализа ситуации, принятия решения в условиях частичной неопределенности и многие другие.

Ход проведения киберучений фиксируется в автоматическом режиме.

Для увеличения вовлеченности и стремления к эффективным действиям реализована функция “быстрой статистики”. В данном блоке могут размещаться оценки преподавателя, показатель эффективности групп в процентах или с использованием любой другой шкалы. Также при наличии ресурсов возможно предусмотреть иные блоки, отражающие статистические данные.

РЕЗУЛЬТАТЫ

Применение киберполигона позволяет продемонстрировать атаки различного типа, необходимые средства защиты.

Реализация разнотипных интерфейсов с узкоспециализированным функционалом даст возможность формирования практических навыков по защите от кибератак у каждого обучаемого.

Группа атакующих улучшит свои знания и навыки в проведении пентестов.

Подгруппа обеспечения эксплуатации сможет получить опыт по настройке и управлению информационной инфраструктурой предприятия в условиях воздействия киберугроз.

Подгруппа мониторинга улучшит свои компетенции по отслеживанию и оценке событий информационной безопасности, анализу киберобстановки, сбору доказательной базы об инциденте.

В свою очередь, подгруппа реагирования на компьютерные инциденты получит опыт по регистрации инцидентов, формированию карточки инцидента и устранению последствий кибератак, восстановлению ресурсов.

Подгруппа форензики отработает навыки по расследованию выявленных кибератак, нахождению причин возникновения инцидентов информационной безопасности, а также поиска нарушителей.

ЗАКЛЮЧЕНИЕ

Использование киберполигона при проведении занятий позволяет обеспечить получение практических навыков, необходимых в профессиональной деятельности. Кроме этого, он может быть использован при реализации программ повышения квалификации в рамках дополнительного профессионального образования.

Работа выполнена при финансовой поддержке гранта МТУСИ, предоставленного Министерством финансов Российской Федерации из федерального бюджета в 2021 г. (научный проект № 35/21-d) в рамках федерального проекта “Информационная безопасность” национальной программы “Цифровая экономика Российской Федерации”.

СПИСОК ЛИТЕРАТУРЫ

1. *Сафонов Н.* Киберполигон – мультифункциональный комплекс для проведения киберучений. https://habr.com/ru/post/80586/
2. *Баранов В.В., Максимова Е.А., Лаута О.С.* // Приборы и системы. Управление, контроль, диагностика. 2019. № 4. С. 32.
3. *Baranov V.V., Maksimova E.A.* // Communications in Computer and Information Science. 2021. № 1395 CCIS, P. 88.
4. *Баранов В.В., Коцыняк М.А., Лаута О.С., Московченко В.М.* // Вестник Волгоградского государственного университета. Сер. 10. Инновационная деятельность. 2017. Т. 11. № 2. С. 11.
5. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006
6. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. http://docs.cntd.ru/document/1200103619
7. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. http://docs.cntd.ru/document/1200103165
8. *Баранов В.В., Максимова Е.А., Зязин В.П.* // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 38.
9. *Алиев Э.Р., Баранов В.В., Игнатьева А.Р.* // Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции “Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации” (Инфобезопасность-2019). Северо-Кавказский федеральный университет. Ставрополь: СКФУ, 2019. С. 30.
10. *Баранов В.В., Коцыняк М.А., Иванов Д.А.* // НБИ Технологии. 2018. Т. 12. № 1. С. 12.