УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 47–53

Сергеев С.С., Баранкова И.И.

DOI: 10.14529/secur220305

МЕТОДИКА ПОСТРОЕНИЯ ГРАФА АТАК ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Нарушение информационной безопасности может быть вызвано рядом причин: наличием уязвимостей в операционных системах и приложениях; неправильной настройкой системы контроля доступа; некорректной настройкой аппаратного и программного обеспечения (далее – ПО); наличием уязвимых сервисов и вредоносного ПО. Используя различные комбинации существующих уязвимостей и слабых мест злоумышленники в зависимости от своих целей могут реализовывать самые разные стратегии атак. Эти стратегии могут быть нацелены на различные критически важные сетевые ресурсы и включают в себя многоэтапные цепочки атак. Поэтому для снижения ущерба от таких инцидентов необходимо обеспечить предотвращение и выявление угроз безопасности, защиту от их воздействия и реагирование на них. Для мониторинга систем можно воспользоваться моделированием, позволяющим получить описание системы и впоследствии производить количественные и качественные оценки ее показателей.

В данной работе будут рассмотрены разработанные подходы и рекомендации для построения графов атак для объектов критической информационной инфраструктуры.

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, объекты критической информационной инфраструктуры, моделирование, граф атак, система защиты информации.*

Sergeev S.S., Barankova I.I.

METHODOLOGY FOR CONSTRUCTING ATTACK GRAPH FOR OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Violation of information security can be caused by a number of reasons: the presence of vulnerabilities in operating systems and applications; incorrect configuration of the access

control system; incorrect configuration of hardware and software (hereinafter referred to as software); the presence of vulnerable services and malware. Using various combinations of existing vulnerabilities and weaknesses, attackers, depending on their goals, can implement a variety of attack strategies. These strategies can target a variety of critical network resources and include multi-stage attack chains. Therefore, in order to reduce the damage from such incidents, it is necessary to ensure the prevention and detection of security threats, protection from their impact and response to them. To monitor systems, you can use modeling, which allows you to get a description of the system and subsequently make quantitative and qualitative assessments of its performance.

This article will consider the developed approaches and recommendations for building attack graphs for critical information infrastructure objects.

Keywords: *information security, critical information infrastructure, objects of critical information infrastructure, modeling, attack graph, information security system.*

Информационные активы предприятия подвержены рискам угроз кибербезопасности из-за использования злоумышленниками некоторых известных уязвимостей. Для снижения ущерба от таких инцидентов необходимо обеспечить предупреждение и выявление угроз безопасности, защиту от их воздействия и реагирование на них. Защита информации, как правило, сочетает в себе использование технических средств и организационных мер. Для мониторинга систем можно использовать математическое моделирование, позволяющее получить формальное описание системы и впоследствии производить количественные и качественные оценки ее показателей.

Выделяются следующие теории, которые могут быть положены в основу моделей СЗИ: теории вероятностей и случайных процессов, теории графов, автоматов и сетей Петри, теория нечетких множеств, теории игр и конфликтов, теория катастроф, эволюционное моделирование, формально-эвристический подход, энтропийный подход.

В данной работе в основу моделирования системы защиты положена теория графов. Алгоритм формирования графа атак предназначен для создания графа атак, описывающего всевозможные варианты реализации атакующих действий нарушителем с учетом его первоначального положения, уровня знаний и умений, исходной конфигурации компьютерной сети и реализуемой в ней политики безопасности. На основе общего графа атак производится анализ защищенности информационной системы, выявляются «узкие» места, формируются рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности и созданию эффективной системы защиты информации [1].

Под эффективностью понимается следование принципу «разумной достаточности», который можно описать следующими утверждениями:

– нельзя создать абсолютно непреодолимую защиту;

– необходимо соблюдать баланс между затратами на защиту и получаемым эффектом;

– стоимость средств защиты не должна превышать стоимости активов;

– затраты нарушителя на несанкционированный доступ к активам должны превосходить эффект в соответствующем выражении, получаемый злоумышленником при осуществлении такого доступа [2].

Граф атак – это визуальное средство, используемое для документирования известных угроз безопасности конкретной архитектуры, он описывает пути, по которым злоумышленники могут достичь своих целей. Применение графов атак позволяет несколько упростить задачу аналитиков при исследовании проблемы безопасности и защищенности [3].

Основной целью данной работы является разработка общих подходов и рекомендаций для построения графов атак для объектов критической информационной инфраструктуры.

Ниже представлены дорожная карта, отображающая этапы моделирования графа атак для объектов КИИ (рис.1).

Для моделирования системы защиты информации и построения графа атак первым этапом необходимо определить структуру объекта, состав технических, программных и программно-аппаратных средств, используемых на объекте КИИ. Также необходимо построить функциональную схему и схему сети

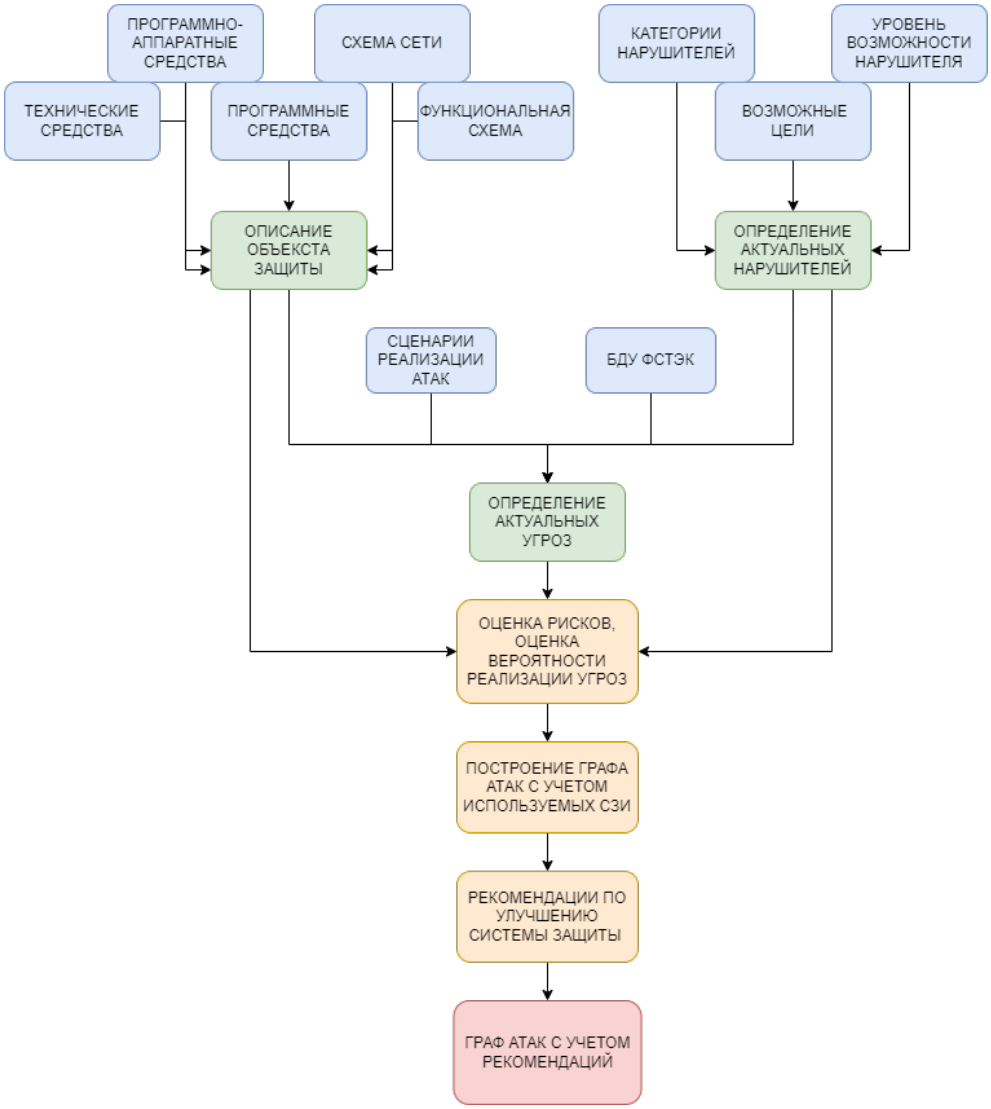

Рис. 1. Дорожная карта построения графа атак для объектов КИИ

объекта. На рисунках 2, 3 приведены примеры, как могут выглядеть функциональная схема и схема сети соответственно.

Следующий этап - выявление возможных нарушителей информационной безопасности в соответствии с Методическим документом «Методика оценки угроз информационной безопасности» (утверждена ФСТЭК России 5 февраля 2021 г.). При определении потенциальных нарушителей следует обратить внимание на следующие категории нарушителей: спецслужбы иностранных государств, террористические группы, преступные группы, хакеры, конкурирующие организации, разработчики программного/программно-аппаратного обеспечения, поставщики программного обеспечения, программно-аппаратных средств, обеспечивающих систем, поставщики услуг связи, вычислительных услуг, лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора, авторизованные пользователи, системные администраторы и администраторы безопасности, бывшие сотрудники [4].

Далее при оценке угроз информационной безопасности должны быть определены возможные пути реализации угроз актуальными нарушителями - актуальные способы реализации угроз информационной безопасности.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. Сценарии реализации угроз информационной безопасности должны быть определены для соответствующих способов реализации угроз безопасности информации и применительно к объектам

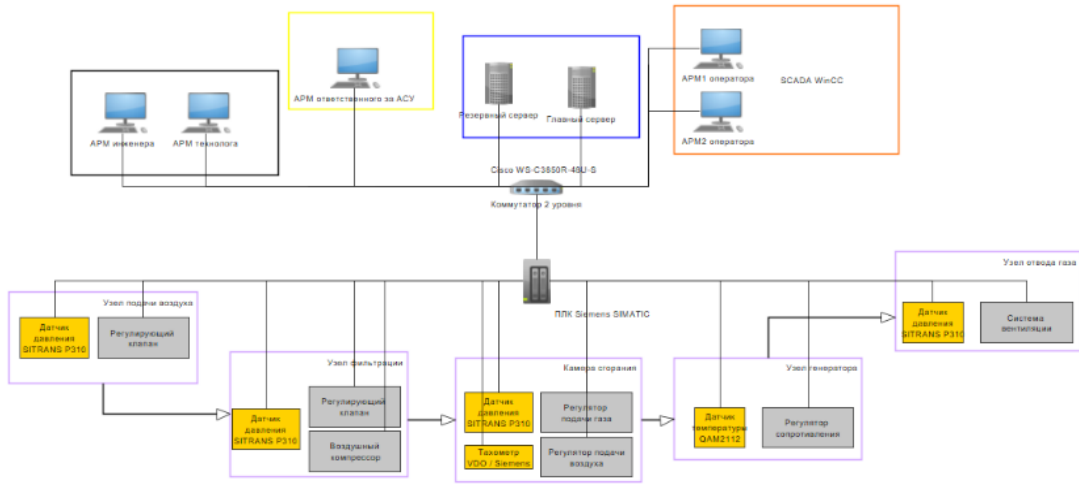

Рис. 2. Пример функциональной схемы АСУ ТП ГТЭС

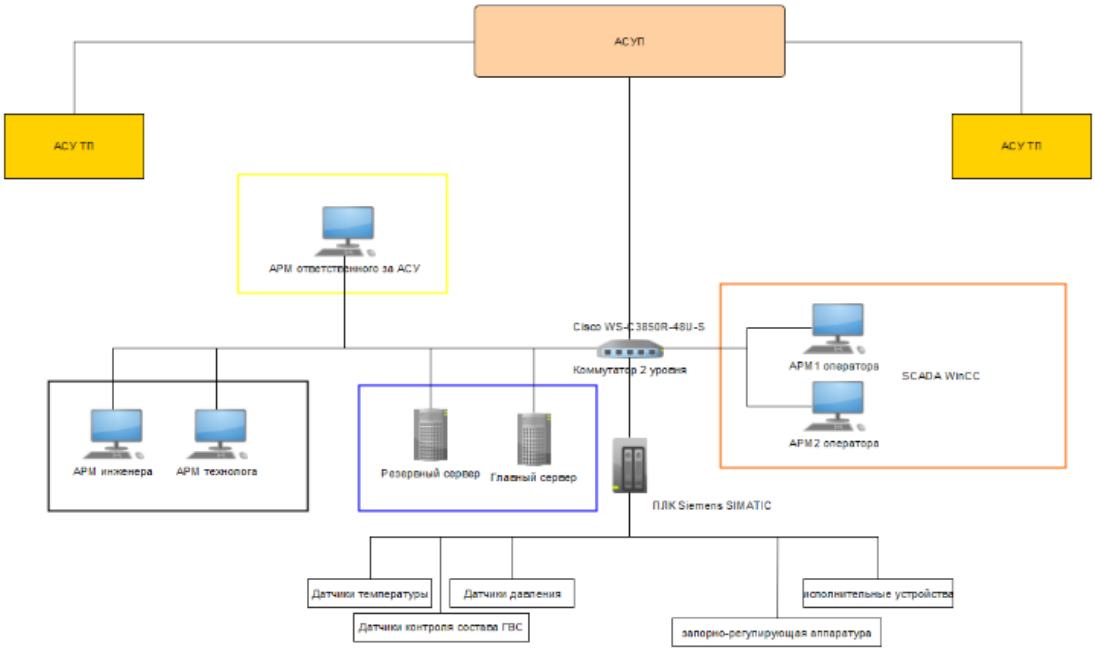

Рис. 3. Пример схемы сети АСУ ТП ГТЭС

воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Следующим важным этапом является оценка рисков. От того, насколько правильно будут оценены риски зависит и эффективность системы информационной безопасности предприятия в целом. Одними из самых распространенных методик управления рисками информационной безопасности являются CRAMM, COBIT for Risk, FRAP, Octave и Microsoft. В [5] приведен краткий обзор методик оценки рисков.

Когда определены актуальные нарушители и их возможности, актуальные угрозы и уязвимости, выполнена оценка рисков, можно строить граф атак.

Алгоритм формирования общего графа атак основан на реализации следующей последовательности действий:

(1) Сбор информации о системах и сетях;

(2) Получение первоначального доступа к компонентам систем и сетей;

(3) Внедрение и исполнение вредоносного программного обеспечения в системах и сетях;

(4) Закрепление в системе или сети;
(5) Управление вредоносным программным обеспечением или компонентами, к которым ранее был получен доступ;

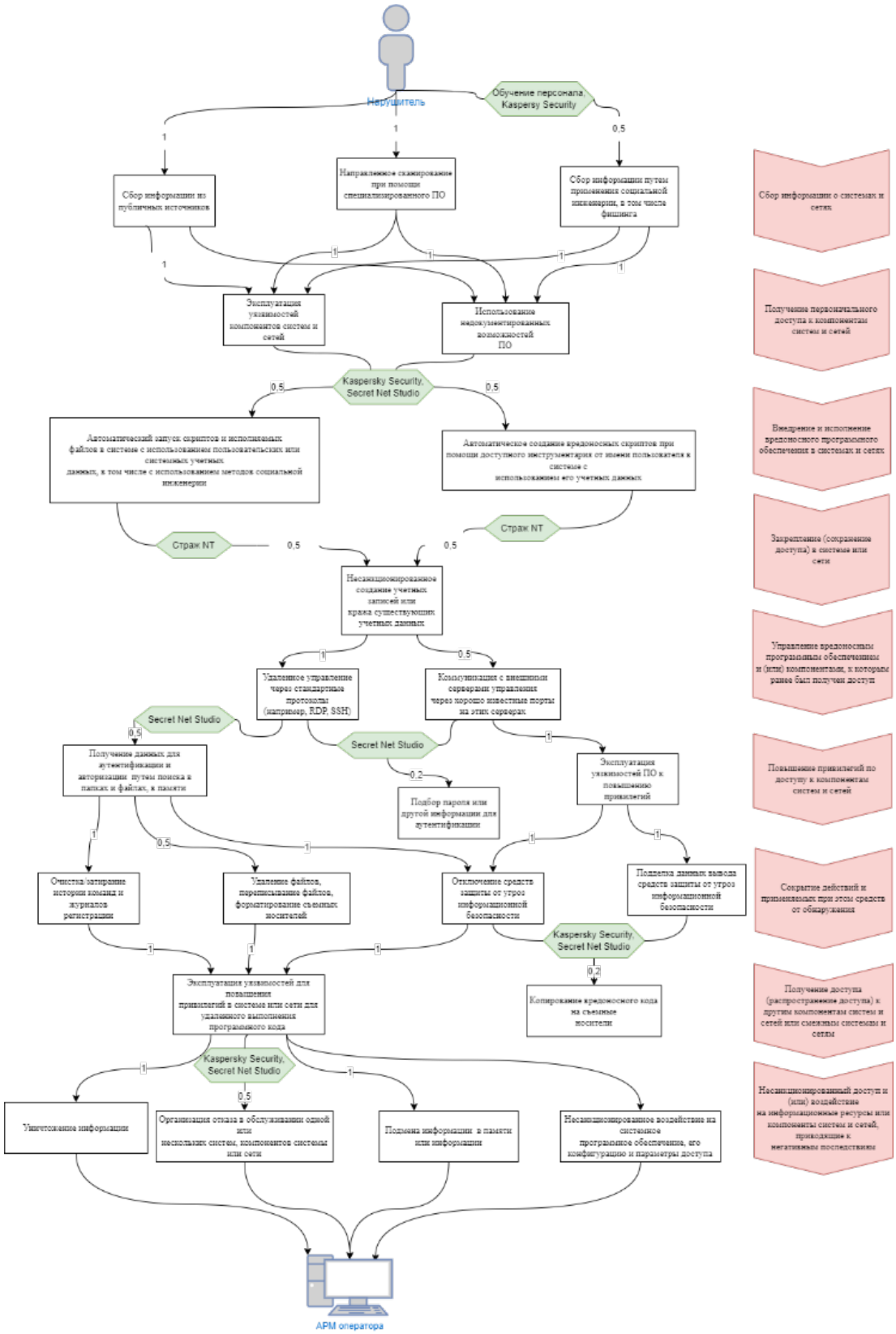

Рис. 4. Граф атак

(6) Повышение привилегий по доступу к компонентам систем и сетей;

(7) Сокрытия действий и применяемых при этом средств от обнаружения;

(8) Получение доступа (распространение доступа) к другим компонентам систем и сетей;

(9) Несанкционированный доступ и негативные воздействие на информационные ресурсы или компоненты систем, сетей [4].

Граф атак нарушителя на АРМ оператора, учитываемый все используемые средства защиты на предприятии приведен на рисунке 4.

На основе построенного графа атак необходимо рассмотреть наиболее вероятно реализуемые сценарии атак и оценить ущерб от их реализации, тем самым определив уязвимые места в системе для дальнейшего формирования рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности и минимизации рисков от происшествий. При формировании рекомендаций по улучшению системы защиты на объектах КИИ также следует учитывать состав мер по обеспечению безопасности для значимого объекта КИИ соответствующей категории значимости, указанный в [6].

Предложенный подход доступно и в полной мере отображает все этапы процесса моделирования системы защиты информации и может быть использован для построения графов атак и выработки рекомендаций для объектов критической информационной инфраструктуры, позволяющие определить уязвимые места в системе и создать эффективную систему защиты информации.

Литература

1. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Построение графа атак для анализа защищенности компьютерных сетей// Символ науки: международный научный журнал. 2016. № 7-2(19). С. 31–32.

2. Курилов Ф.М. Моделирование систем защиты информации. Приложение теории графов / Ф.М. Курилов. – Текст: непосредственный // Технические науки: теория и практика: материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). – Чита: Издательство Молодой ученый, 2016. – С. 6–9.

3. Баранкова И.И., Михайлова У.В., Афанасьева М.В. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности// Динамика систем, механизмов и машин. 2019. №4. С. 60–66

4. Методический документ методика оценки угроз безопасности информации [Текст], Утвержден ФСТЭК России 5 февраля 2021 г. – 2021. – 83 с.

5. Гаврилов А.В., Сизов В.А., Ярошенко Е.В. Методика оценки рисков информационной безопасности предприятия с использованием CASE-технологий// Open education. 2021. № 5. С. 41–49.

6. Приказ ФСТЭК России N 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации" [Текст], Утвержден ФСТЭК России 25 декабря 2017 г. – 2017. – 37 с.

References

1. Alekseev D.M., Ivanenko K.N., Ubiraylo V.N. Postroenie grafa atak dlya analiza zashchishchennosti komp'yuternykh setey// Simvol nauki: mezhdunarodnyy nauchnyy zhurnal. 2016. № 7-2(19). P. 31–32.

2. Kurilov F.M. Modelirovanie sistem zashchity informatsii. Prilozhenie teorii grafov / F.M. Kurilov. – Tekst: neposredstvennyy // Tekhnicheskie nauki: teoriya i praktika: materialy III Mezhdunar. nauch. konf. (g. Chita, aprel' 2016 g.). – Chita: Izdatel'stvo Molodoy uchenyy, 2016. – P. 6–9.

3. Barankova I.I., Mikhaylova U.V., Afanas'eva M.V. Minimizatsiya riskov informatsionnoy bezopasnosti na osnove modelirovaniya ugroz bezopasnosti// Dinamika sistem, mekhanizmov i mashin. 2019. №4. P. 60–66.

4. Metodicheskiy dokument metodika otsenki ugroz bezopasnosti informatsii [Tekst], Utverzhden FSTEK Rossii 5 fevralya 2021 g. – 2021. – 83 p.

5. Gavrilov A.V., Sizov V.A., Yaroshenko E.V. Metodika otsenki riskov informatsionnoy bezopasnosti predpriyatiya s ispol'zovaniem CASE-tekhnologiy// Open education. 2021. № 5. P. 41–49.

6. Prikaz FSTEK Rossii N 239 "Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury rossiyskoy federatsii" [Tekst], Utverzhden FSTEK Rossii 25 dekabrya 2017 g. – 2017. – 37 p.

СЕРГЕЕВ Сергей Сергеевич, студент 5 курса по специальности «Информационная безопасность автоматизированных систем», ФГБОУ ВО «Магнитогорский государственный техни-

ческий университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: sergeyjek@yandex.ru

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

SERGEEV Sergey Sergeevich, 5th year student majoring in "Information Security of Automated Systems", Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: sergeyjek@yandex.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru