



Васильев В. И., Кириллова А. Д., Сагитова В. В.

ОБ ЭВОЛЮЦИИ ПОНЯТИЯ «ПРОФИЛЬ ЗАЩИТЫ» В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализируется понятие профиля защиты, выступающее сегодня в качестве одного из ключевых понятий при построении и оценке эффективности систем защиты информации. Отмечается основополагающая роль стандарта ГОСТ Р ИСО/МЭК 15408 в формировании и конкретном наполнении данного понятия применительно к различным классам ИТ-продуктов и систем. Обсуждаются возможные подходы к разработке и применению профилей защиты с учетом требований базовых руководящих документов Федеральной службы по техническому и экспертному контролю (ФСТЭК) России. Рассматриваются возможности расширения данного понятия на задачи обеспечения комплексной безопасности предприятий (организаций).

Ключевые слова: информационная безопасность, защита информации, профиль защиты, системы обеспечения комплексной безопасности.

Vasilyev V. I., Kirillova A. D., Sagitova V. V.

ON EVOLUTION OF «PROTECTION PROFILE» NOTION IN THE SPHERE OF INFORMATION SECURITY

The notion of protection profile being now one of the key notions in developing and evaluating the information security systems is analyzed. The fundamental role of the standard GOST R ISO/IEC 15408 in forming and filling this notion applied to different classes of IT-products and systems is noted. Possible approaches to development and application of protection profiles with account of basic ruling documents by Federal Service on Technical and Expert Control (FSTEC) of Russia are discussed. The opportunities of extending this notion to the problems of providing the complex security for enterprises (organizations) are considered.

Keywords: information security, information protection, protection profile, complex security provision systems.

Проблемы информационной безопасности (ИБ) сегодня непосредственно касаются всех сфер нашей жизни, так или иначе связанных с применением информационных технологий (ИТ). Как свидетельствует статистика [1], рост числа угроз и уязвимостей при этом сопровождается увеличением суммарного ущерба от реализации этих угроз, объектами которых являются промышленные предприятия, государственные и коммерческие организации, медицинские и образовательные учреждения и т.п. Очевидно, что для эффективного противодействия этой тенденции необходимо комплексное применение на каждом объекте системы организационно-технических мер и мероприятий, опирающееся на

ний безопасности, которым должны удовлетворять программно-аппаратные средства и/или системы определенного класса (обобщенно – объект оценки). Задание по безопасности – это совокупность требований к конкретной разработке, выполнение которых позволит решить поставленные задачи по обеспечению безопасности.

Профиль защиты (ПЗ) не регламентирует, каким образом должны выполняться заложенные в нем требования, тем самым предоставляя возможность разработчику системы защиты информации (СЗИ) самостоятельно выбирать средства защиты. Согласно [3], требуемое содержание ПЗ должно включать в себя следующие разделы (таблица 1).

Таблица 1

Профиль защиты

Раздел ПЗ	Содержание раздела
Введение	Идентификация ПЗ. Аннотация
Описание объекта оценки (ОО)	Границы среды безопасности. Угрозы активам, требующим защиты (включая описание этих активов). Политика безопасности организации.
Цели безопасности	Цели безопасности ОО. Цели безопасности среды.
Требования безопасности	Функциональные требования. Требования доверия к безопасности. Требования безопасности ИТ-среды ОО.
Обоснование ПЗ	Убедительные аргументы в пользу того, что рекомендуемые требования безопасности ИТ удовлетворяют намеченным целям безопасности с учетом всех аспектов среды безопасности.

научно-обоснованную нормативно-законодательную базу в области защиты информации (ЗИ) и имеющее своей конечной целью снижение уровня ожидаемых информационных рисков. Важное место при разработке комплекса таких мер и мероприятий имеют обоснованное задание требований к безопасности ИТ-продуктов и систем, оценка безопасности и возможность проведения сравнительного анализа уровня безопасности ИТ-продуктов и систем с использованием такого ключевого понятия ИБ, как профиль защиты.

История происхождения данного понятия связана прежде всего с международным стандартом ISO/IEC 15408-3-1999 («Общие критерии») и его российским аналогом (последняя версия ГОСТ Р ИСО/МЭК 15408-3-2008 [2]), где в качестве 2-х видов базовых нормативных документов, определяющих требования к безопасности ИТ-продуктов и систем, выделены **профиль защиты** (Protection Profile) и **задание по безопасности** (Security Target). В соответствии с [2], профиль защиты – это типовой набор требова-

На сегодняшний день ФСТЭК России разработала и утвердила около 100 методических документов, содержащих ПЗ для различных ИТ-продуктов и систем [4], в том числе:

- ПЗ систем обнаружения вторжений;
- ПЗ межсетевых экранов;
- ПЗ средств антивирусной защиты;
- ПЗ операционных систем;
- ПЗ средств контроля отчуждения (переноса) информации со съемных машинных носителей информации;
- ПЗ средств доверенной загрузки уровня базовой системы ввода-вывода; и др.

Большая часть этих ПЗ согласуется с международной трактовкой понятия ПЗ, жестко привязанной к исходному стандарту ISO/IEC 15408 и его аналогов-национальных стандартов. В частности, предполагается, что входящие в ПЗ требования безопасности (функциональные требования, требования доверия и т.п.) должны заимствоваться только из приведенного в этих стандартах перечня типовых требований. В то же время, в последние годы получает все большее распространение точ-

ка зрения, что при таком подходе невозможны унификация, регламентирование и параметризация множества конкретных функций и характеристик сложных объектов архитектуры и структуры современных информационных систем (ИС) [5]. Отсюда понятен интерес к внедрению нового прагматического подхода к разработке и применению ПЗ, основанного на использовании совокупности адаптированных и параметризованных баз международных и национальных стандартов и открытых спецификаций, отвечающих стандартам де-факто и нормативных документов ведущих фирм (компаний).

Одним их преимуществ ПЗ является возможность их использования для проведения аудита ИБ ИС. В качестве примера подобного применения ПЗ можно привести предложенную в [6] методику оценки эффективности СЗИ ИСПДн с учетом ПЗ, построенного на базе стандарта ГОСТ Р ИСО/МЭК ТО 19791 [7]. Данный стандарт включает в себя определение и модель автоматизированной (информационной) системы, описание расширенной концепции оценки безопасности системы, методологию и процесс выполнения оценки безопасности системы, а также дополнительные критерии оценки безопасности. Требования стандарта базируются на 3-этапном подходе к обеспечению необходимого уровня безопасности системы:

- оценка рисков безопасности;
- уменьшение рисков посредством выбора контрмер;
- аттестация для подтверждения приемлемого уровня остаточных рисков.

В качестве базовых нормативных документов при разработке ПЗ ИС могут быть использованы руководящие документы ФСТЭК России, устанавливающие перечень требований по обеспечению безопасности различных классов ИС, таких как государственные информационные системы (ГИС) [8], информационные системы персональных данных (ИСПДн) [9], автоматизированные системы управления производственными и технологическими процессами (АСУ ТП) [10], значимые объекты критической информационной инфраструктуры Российской Федерации [11]. В каждом из этих документов, в основу которых положены ГОСТ Р ИСО/МЭК 15408-2008 и ГОСТ Р ИСО/МЭК 27001-2006, определены группы типовых требований к ЗИ, которые затем конкретизируются (уточняются) для каждой из этих групп. Оценивая степень выпол-

нения (или невыполнения) указанных требований для конкретной ИС с помощью оценочных показателей (критериев), значения которых выставляются экспертом или группой экспертов, можно получить некоторое интегральное представление о фактическом («достигнутом») ПЗ и его соответствие «эталонному» ПЗ ИС [12, 13].

Рассмотрим ситуацию, связанную с построением ПЗ, на примере АСУ ТП [14]. Приказ ФСТЭК № 31 содержит 21 группу типовых требований (мер ЗИ в АСУ ТП), каждая из которых включает в себя от 3 до 31 конкретных требований (мер защиты), в зависимости от требуемого класса защищенности системы. Обозначим через M_{ij} частный показатель степени выполнения j -го требования ($j=1,2,\dots,n_i$) в i -й группе требований ($i=1,2,\dots,21$). Будем полагать, что $M_{ij}=0$, если соответствующее требование не выполняется; $M_{ij}=0,5$, если данное требование выполняется частично (не в полной мере) и $M_{ij}=1$, если это требование реализовано в полном объеме. Тогда для каждой (i -ой) группы требований можно вычислить групповой показатель степени выполнения заданного набора требований EV_i , выраженный в %, и абсолютный показатель NE_i числа нереализованных или частично реализованных требований к ЗИ, относящихся к i -й группе:

$$EV_i = \left(\frac{1}{n_i} \sum_{j=1}^{n_i} M_{ij} \right) \cdot 100\%; \quad NE_i = n_i - \sum_{j=1}^{n_i} unit(M_{ij}), \quad (1)$$

где функция $unit(M_{ij})$ равна 1, если $M_{ij}=1$, и 0, если $M_{ij}=0$ или 0,5; n_i – число требований к ЗИ в i -й группе требований. Так, если некоторая группа требований (например, 1-ая – «Идентификация и аутентификация субъектов доступа и объектов доступа») включает в себя 8 требований (базовых мер защиты), из которых в конкретной системе полностью реализованы 6 требований, частично – 1 и не выполнено 1 требование, то имеем: $n_i=8$; $EV_i=81,3\%$; $NE_i=2$.

На рисунке 1 приведен пример линейчатой диаграммы ПЗ, показывающей значения всех 21 групповых показателей EV_i и NE_i для некоторой АСУ ТП.

Анализ полученной диаграммы ПЗ позволяет оценить общий уровень защищенности АСУ ТП, выявить слабые места в системе ЗИ, наметить конкретные меры для реализации требований ФСТЭК по обеспечению безопасности АСУ ТП в полном объеме.

Дальнейшее развитие концепции ПЗ свя-



Рис.1 Диаграмма групповых показателей степени выполнения требований ПЗ (●●● EV_i; ■■■ NE_i)

зано с расширением этого понятия на задачи обеспечения комплексной безопасности предприятия (организации). В [15] под профилем защиты предприятия (объекта транспортной инфраструктуры) понимается типовой состав требований по обеспечению безопасности объекта и реализующего эти требования комплекса средств и мероприятий, обеспечивающих приемлемый уровень безопасности всего множества объектов данной категории и данного вида транспорта. Работа [16] посвящена общим методологическим вопросам построения систем обеспечения безопасности (СОБ) критически важных объектов (КВО) на базе формирования и оценки профиля защиты КВО. Под профилем защиты КВО при этом понимается независимая от реализации угроз совокупность требований безопасности для каждого типа КВО, обеспечивающая достаточную степень его защищенности. Как отмечают авторы [16], в общем случае возможны следующие постановки задачи обеспечения безопасности КВО:

1) определить эффективность функционирования СОБ при заданной модели угроз и существующем профиле защиты КВО;

2) при заданной модели угроз определить профиль защиты КВО, обеспечивающей минимальную стоимость средств защиты при допустимом уровне риска нарушения его безопасности;

3) определить профиль защиты КВО, обеспечивающий максимальный уровень безопасности объекта при заданной стоимости средств защиты.

Конструктивное определение близкого по своему смыслу и содержанию понятия «профиль безопасности объекта» вводится в [17]. По мнению автора, профиль безопасности должен включать в себя следующие разделы:

1) политика безопасности объекта – совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности;

2) уровень безопасности объекта – совокупность нормативно-правовых, программно-технических и физических средств/систем защиты объекта, обеспечивающих противодействие угрозам несанкционированного доступа;

3) система аудита безопасности – совокупность методов и средств, позволяющих дать оценку проектируемой (анализируемой) системы с использованием определенного перечня оценочных критериев.

В развитие идей, изложенных в [16, 17], следует отметить, что комплексная СОБ объекта – это сложная многокомпонентная система, в силу разнородности решаемых ей задач и выполняемых ею функций состоящая из ряда относительно самостоятельных подсистем безопасности, интегрированных на основе общей информационной среды с единой базой данных. В качестве таковых подсистем обычно выступают подсистемы, отвечающие за:

- информационную безопасность;
- функциональную надежность выполнения бизнес-процессов (безопасность АСУ ТП);
- физическую защиту объекта;
- уровень квалификации и технологической дисциплины персонала;
- управление в чрезвычайных (нештатных) ситуациях.

Очевидно, что разработка системы оценочных критериев (метрик безопасности), позволяющих в полной мере оценить эффективность функционирования указанных подсистем в составе СОБ для достижения главной поставленной цели – обеспечение безопасности объекта в условиях воздействия внешних и внутренних угроз – пока еще далека от своего разрешения.

В наиболее общей постановке проблема формирования профилей интегрированных систем обеспечения комплексной безопасности (ИСОКБ) на примере предприятий наукоемкого машиностроения рассмотрена в монографии [18]. В соответствии с предложенной в этой работе концепцией, структурно ИСОКБ предприятия может быть представлена в виде спецификации программно-технических и программно-методических комплексов, образующих сложную организационно-техническую систему. В качестве профиля ИСОКБ предприятия в данном случае рассматривается упорядоченный и ограниченный набор стандартов, спецификаций требований к компонентам этой системы и

описания основных проектных решений, используемых для обеспечения безопасности бизнес-процессов предприятия. В состав базового профиля ИСОКБ предприятия при этом входят:

– описание основных компонент ИСОКБ предприятия, включая определение объектов и субъектов безопасности, процессы мониторинга и идентификации инцидентов – угроз безопасности;

– общесистемные требования к формированию информационной среды и распределенных служб обеспечения безопасности;

– требования к процессам обработки и представления данных для принятия решений на разных уровнях управления.

Достоинствами предложенного в [18] подхода является увязка целей, задач и архитектуры проектируемой ИСОКБ со спецификой бизнес-процессов предприятия, рассмотрение с единых системных позиций всех этапов жизненного цикла ИСОКБ, возможность автоматизированного анализа и проектирования профиля ИСОКБ современного предприятия, внедрение которой позволит обеспечить его безопасное функционирование и устойчивое развитие.

Подводя итоги вышесказанному, можно

сделать следующие выводы. Понятие ПЗ является конструктивным и полезным в современных условиях развития ИТ, т.к. его использование дает в руки различных категорий лиц (разработчики, пользователи, аудиторы) нормативный документ, содержащий базовые требования к тому или иному классу ИТ-продуктов и систем. Сфера разработки и применения ПЗ постоянно расширяется, охватывая не только узкоспециализированные ИТ-продукты (системы обнаружения вторжений, межсетевые экраны, средства антивирусной защиты и др.), но и ИС различного назначения. Внедрение в повседневную практику руководящих документов ФСТЭК России способствует этой тенденции, иницируя разработку ПЗ для таких классов ИС, как ИСПДн, ГИС, АСУ ТП, КВО. Очередным шагом в развитии ПЗ является построение ПЗ объектов (предприятий, организаций), приводящее в конечном итоге к созданию и внедрению интегрированных систем обеспечения комплексной безопасности этих объектов.

Статья выполнена при поддержке гранта РФФИ № 17-48-020095 «Разработка концептуальных основ и методологии математического моделирования систем обеспечения комплексной безопасности промышленных объектов».

Литература

1. Зинина О. Анализ угроз информационной безопасности 2016-2017. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security_threats_2016_2017 (дата обращения: 18.05.2018).
2. ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Часть 3. Требования доверия к безопасности. – М.: Стандартинформ, 2009.
3. ГОСТ Р ИСО/МЭК ТО 15446-2008. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. – М.: Стандартинформ, 2010.
4. Техническая защита. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации / Методический документы. Утв. ФСТЭК России 11 мая 2017 г. URL: <https://fstec.ru/technicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty> (дата обращения: 18.05.2018).
5. Липаев В., Филинов Е. Формирование и применение профилей открытых информационных систем // Открытые системы. СУБД, № 5, 1997. URL: <https://www.osp.ru/os/1997/05/179274> (дата обращения: 18.05.2018).
6. Селифанов В.В., Звягинцева П.А., Голдобина А.С., Исаева Ю.А. Оценка эффективности системы защиты информации ИСПДн с учетом профиля защиты // Интерэкспо Гео-Сибирь, т.8, 2017. – С. 220-225.
7. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. – М.: Стандартинформ, 2010.
8. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах / Утв. Приказом ФСТЭК России № 17 от 11.02.2013 г.
9. Состав и содержание организационных и технических мер по обеспечению безопасности пер-

сональных данных при их обработке в информационных системах персональных данных / Утв. Приказом ФСТЭК России № 21 от 18.02.2013 г.

10. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды / Утв. Приказом ФСТЭК России № 31 от 14.03.2014 г.

11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Утв. Приказом ФСТЭК России № 239 от 25.12.2017 г.

12. Замула А.А., Северинов А.В., Корниенко М.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации // Наука і техніка Повітряних Сил Збройних Сил України, № 2 (15), 2014. – С. 133-138.

13. Датская Л.В., Кожевникова И.С., Ананьин Е.В., Оладько В.С. Автоматизация проведения аудита информационной безопасности на основе профиля защиты // Национальная ассоциация ученых (НАУ), № VI (11), 2015. Технические науки. – С. 18-22.

14. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами // Инфокоммуникационные технологии, – 2017. – т.5. – №4. – С. 319-326.

15. Стилиславский А.Б. Построение профилей защиты категоризируемых объектов транспортной инфраструктуры // Информационные технологии и вычислительные системы. – 2009. – №4. – С. 77-83.

16. Нечаев Д.Ю., Черешкин Д.С. Методологические аспекты интеграции систем обеспечения безопасности критически важных объектов // Изв. Российского экономического ун-та им. Г.В. Плеханова: Электронный научный журнал, № 2 (20), 2015. URL: [https://www.rea.ru/ru/org/managements/izdcentr/Pages/2\(20\),2015.aspx](https://www.rea.ru/ru/org/managements/izdcentr/Pages/2(20),2015.aspx) (дата обращения: 18.05.2018).

17. Маликов В.В. Профили безопасности объектов различных форм собственности // Доклады БГУИР. – 2009. – № 2 (40). – С. 99-104.

18. Прохоров С.А., Федосеев А.А., Денисов В.Ф., Иващенко А.В. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения. – Самара: Самарский научный центр РАН, 2009. – 199 с.

References

1. Zinina O. Analysis of information security threats. Available at: URL:https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security_threats_2016_2017 (accessed 18 May 2018).

2. GOST R ISO/IEC 15408-3-2008 Information technology. Security techniques Evaluation criteria for IT security. Part 3. Security assurance requirements. Moscow, Standartinform, 2009.

3. GOST R ISO/IEC TO 15446-2008 Information technology (IT). Security techniques. Guide on development of protection profiles, Moscow, Standartinform, 2010.

4. Technical protection. Documents on certification of information protection tools and evaluation of informatization objects by information security requirements / Methodical documents. Appr. by FSTEC of Russia 11 May, 2017. Available at: <https://fstec.ru/technicheskaya-zashchita-informatsii/dokumenty-posertifikatsii/120-normativnye-dokumenty> (accessed 18 May 2018).

5. Lipaev V., Filinov E. Formation and application of open information systems profiles. Available at: <https://www.osp.ru/os/1997/05/179274> (accessed 18 May 2018).

6. Selifanov V.V., Zvyagintseva P.A., Goldobina A.S., Isaeva Yu.A. Evaluation of PDIS information protection system efficiency with account of protection profile. Interexpo Geo-Sibir, v.8, 2017. P. 220-225.

7. GOST R ISO/IEC TO 19791-2008 Information technology. Security techniques. Evaluation of automated systems security. Moscow, Standartinform, 2010.

8. Requirements on protection of information not being the state mystery, containing in state information systems. Appr. by the Order of FSTEC of Russia №17 of 11.02.2013.

9. Composition and content of organizational and technical measures by providing security of private data under their processing in information systems of private data. Appr. by the Order of FSTEC of Russia № 21 of 18.02.2013.

10. Requirements on providing information protection in automated control systems of production and technological processes at critically important objects, potentially dangerous objects, and also objects representing high danger to human life and health and to natural environment / Appr. by the Order of FSTEC of Russia № 31 of 14.03.2017.

11. Requirements on providing security of significant objects of critical information infrastructure of Russian Federation / Appr. by the Order of FSTEC of Russia № 239 of 25.12.2017.

12. Zamula A.A., Severinov A.V., Kornienko M.A. Analysis of evaluation models of information security risks for constructing information security systems / *Nauka i tekhnika Povitryanykh Sil Zbroinykh Sil Ukrainy*, № 2 (15), 2014. P. 133-138.

13. Datskaya L.V., Kozhevnikova I.S., Ananyin E.V., Oladko V.S. Automatization of conducting information security audit on the basis of protection profile / *National scientists association (NSA)*, № VI (11), 2015. Technical Sciences. P. 18-22.

14. Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kirillova A.D. Complex evaluation of carrying out requirements to providing information protection in automated control systems of production and technological processes / *Infocommunicational technologies*, v.5., №4, 2017. P. 319-326.

15. Stislavsky A.B. Construction of protection profiles for categorized objects of transport infrastructure / *Information technologies and computer systems*, №4, 2009. P. 77-83.

16. Nechaev D.Yu., Chereskin D.S. Methodological aspects of integrating security provision systems for critically important object / *Proceedings of Russian Economical University by mane G.V. Plekhanov: Electronic scientific journal*, № 2 (20). Available at: [https://www.rea.ru/ru/org/managements/izdcentr/Pages/2\(20\),2015.aspx](https://www.rea.ru/ru/org/managements/izdcentr/Pages/2(20),2015.aspx) (accessed 18 May 2018).

17. Malikov V.V. Security profiles for different property forms objects / *BGUIR Transactions*, 2009, № 2 (40), P. 99-104.

18. Prokhorov S.A., Fedoseev A.A., Denisov V.F., Ivashenko A.V. Methods and tools of designing profiles of integrated systems of complex security provision for enterprises of scientific machine-building. Samara, Samara Scientific Center of RAN, 2009. 199 p.

ВАСИЛЬЕВ Владимир Иванович, доктор технических наук, профессор кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: vasilyev@ugatu.ac.ru.

КИРИЛЛОВА Анастасия Дмитриевна, магистр, программист кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kirillova.andm@gmail.com

САГИТОВА Валентина Владимировна, аспирант кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: sagitovavv@mail.ru

VASILYEV Vladimir, Dr. Sc. (Eng.), Professor of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: vasilyev@ugatu.ac.ru.

KIRILLOVA Anastasiya, M. Sc., programmer of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: kirillova.andm@gmail.com

SAGITOVA Valentina, post-graduate of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: sagitovavv@mail.ru