

МИНИСТЕРСТВО ОБРАЗОВАНИЯ
И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ (РИНХ)

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы VI Всероссийской научной конференции
21-22 декабря 2016 года

Ростов-на-Дону
2016

УДК 378 + 00.4.056

ББК 65.050.2

П 78

П 78 Проблемы информационной безопасности : материалы VI Всероссийской научной конференции, 21-22 декабря 2016 года. – Ростов н/Д: Издательско-полиграфический комплекс РГЭУ (РИНХ), 2016. – 200 с.

ISBN 978-5-7972-2298-9

В издании представлены работы профессорско-преподавательского состава, молодых ученых, магистров и студентов, посвященные проблемам информационной безопасности.

Материалы конференции предназначены для научных сотрудников, преподавателей, аспирантов, магистров и студентов.

Редакционная коллегия

Тищенко Е.Н. (ответственный редактор), члены редколлегии

Богачев Т.В., Шейдаков Н.Е., Скляр А.В.

Утверждены в качестве материалов конференции редакционно-издательским советом РГЭУ (РИНХ).

ISBN 978-5-7972-2298-9

© Ростовский государственный
экономический университет (РИНХ), 2016

<i>Корабельщикова С.Ю., Попович И.В.</i>	
Оценка максимальных размеров двоичных кодов, исправляющих ошибку	155
<i>Могилевская Н.С., Поляков А.О., Тибекина К.Б.</i>	
Модификация статистического метода распознавания авторства текстов с использованием частот k-грамм и исследование его эффективности	159
Секция 6. Комплексное обеспечение	
информационной безопасности	159
<i>Ажмухамедов И.М., Носиров З.А.</i>	
Модифицированная беспроводная охранная система Wireless Security.....	164
<i>Василишин И.И., Ипатов Ю.Л., Пугин М.С., Султанов Д.М.-М.</i>	
Проект автономного шифровального устройства, реализующего российский стандарт блочного криптографического преобразования ГОСТ Р 34.12-2015	167
<i>Гостюнина В.А.</i>	
«Родительский контроль» – важный инструмент для безопасного интернета.....	172
<i>Красноперова А.А., Ажмухамедов А.И., Кипарисова А.И.</i>	
Управление персоналом с целью снижения уровня антропогенных угроз	176
<i>Марьенков А.Н., Гудонис В.М.</i>	
Обеспечение безопасности персональных данных при электронном документообороте между удостоверяющим центром и его клиентами.....	180
<i>Харечкин П. В.</i>	
Исследование угроз информационной безопасности робототехническим комплексам	184
Наши авторы	189

3. Кульба В.В., Малюгин В.Д., Шубин А.Н. Информационное управление (предпосылки, методы и средства) // Проблемы управления. 2003. №1. С. 62-67;

Марьенков А.Н., Гудонис В.М.

**Обеспечение безопасности персональных данных
при электронном документообороте
между удостоверяющим центром и его клиентами**

В настоящее время юридически значимый электронный документооборот используется все шире. При этом, для придания электронному документу юридической значимости используется механизм электронной подписи.

Главным нормативно-правовым документом, регламентирующим условия использования электронной подписи на территории Российской Федерации, является Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». В нем выделены три разновидности электронной подписи: простая, усиленная неквалифицированная и усиленная квалифицированная. Простая электронная подпись сформирована с помощью конфиденциального ключа и содержится в самом электронном документе, тем самым подтверждая сам факт формирования электронной подписи. Усиленная неквалифицированная электронная подпись должна быть сформирована с помощью криптографического средства электронной подписи и ключа электронной подписи, которые обеспечивают возможность ее проверки, в также обнаружение факта изменения электронного документа. Усиленная квалифицированная электронная подпись обязательно используется с сертификатом ключа проверки электронной подписи, созданным только удостоверяющим центром, аккредитованным уполномоченным федеральным органом в отношении удостоверяющих центров. Документ, подписанный действующей электронной подписью, обладает равной с традиционным бумажным документом правомочностью.

Таким образом, для получения электронной подписи гражданину необходимо обратиться в один из аккредитованных удостоверяющих центров, предоставив ряд документально подтвержденных данных, которые перечислены в Федеральном Законе «Об электронной подписи», а также за-

ключить договор на оказание услуг по выпуску электронной подписи. В настоящее время удостоверяющие центры собирают эту информации на бумажных носителях. Такой подход долг, трудоемок, и приводит к большому времени ожидания ответной реакции, даже в случае, когда клиент подает все документы правильно заполненными с первого раза. Если же рассматривать намного более часто встречающийся случай, при котором клиент совершает ошибки, то время- и трудозатраты значительно увеличиваются.

Чтобы уменьшить данные недостатки, некоторые удостоверяющие центры предлагают предварительно отправлять им через информационно-телекоммуникационную сеть все необходимые данные, чтобы совместно с клиентом подготовить необходимый набор документов. Сам выпуск происходит при получении подписанных бумажных оригиналов документов.

Такой подход, хоть и значительно ускоряет процесс, но вносит определенный элемент дублирования при оформлении и проверке документов. Максимально избавиться от этого недостатка можно, если подаваемые клиентом документы в электронном виде будут подписаны электронной подписью, выданной ему ранее. Таким образом, подаваемые документы получают юридическую значимость и пропадет необходимость в их повторной подаче в удостоверяющий центр на бумажных носителях. В данном случае, пакет документов на бумажном носителе необходим только при получении клиентом своей первой электронной подписи.

Для реализации юридически значимого документооборота между удостоверяющими центрами и их клиентами предлагается создать информационную систему, которая принимала бы от пользователя заявление на оказание нужной услуги и все необходимые для этого данные и автоматически генерировала соответствующие документы, позволяя подписывать пакет документов электронной подписью и подавать в электронном виде, а также давая возможность вывода документов на печать.

Очевидно, что в данной системе будет обрабатываться большой объем персональных данных клиентов удостоверяющего центра. В соответствии с действующим законодательством такая информационная система должна быть защищена согласно требованиями, утвержденным Постановлением Правительства РФ от 01.11.2012 № 1119.

Для того чтобы узнать конкретный перечень обязательных (в зависимости от конкретных параметров системы) для реализации мер защиты,

рассмотрим классификацию данной информационной системы. Для этого определим категорию обрабатываемых персональных данных, количество субъектов, данные которых будут обрабатываться и тип угроз информационной системы. Также сразу заметим, что обрабатываться будут персональные данные субъектов, не являющихся сотрудниками оператора. Категорию персональных данных определим, как иные персональные данные, так как они не относятся ни к специальным, ни к биометрическим, ни к общедоступным. Рассматриваемый тип угроз – третий. К нему относятся угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. Таким образом согласно Постановлению Правительства РФ от 01.11.2012 № 1119 для рассматриваемой информационной системы будет необходимо обеспечить 4-й или 3-й уровень защищенности персональных данных, в зависимости от того, обрабатываются персональные данные меньше или больше чем 100 000 субъектов соответственно.

В соответствии с Приказом ФСТЭК от 18.02.2013 г. № 21 информационная система персональных данных 4-го уровня защищенности должна включать в себя перечень мер и механизмов защиты, содержащий 27 наименований, которые перечислены в Приложении к данному Приказу.

Информационная система персональных данных 3-го уровня защищенности помимо вышеперечисленного должна также включать в себя еще 14 позиций, также перечисленных в Приложении к Приказу

В случае, если информационная система, обеспечивающая электронный документооборот между удостоверяющим центром и его клиентами, является подсистемой государственной информационной системы, то она должна соответствовать требованиям Приказа ФСТЭК России от 11.02.2013 г. № 17. Чтобы узнать конкретный перечень требований нужно определить класс защищенности информационной системы. Он зависит от масштаба информационной системы (федеральный, региональный, объектовый) и уровня значимости, обрабатываемой в ней информации. Последний в свою очередь отражает степень возможного ущерба в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности). Ущерб может быть высоким, средним, низким или неопределенным (но явно незначительным) и в зависимости от

его величины информации присваивается уровень значимости от 1-го (высокий ущерб) до 4-го (незначительный).

Для рассматриваемой информационной системы не имеет смысла выносить какие-либо из ее сегментов за пределы объектов удостоверяющего центра, так как хранить и обрабатывать поступающую информацию намного безопасней и дешевле централизованно, поэтому далее будем рассматривать информационную систему объектового масштаб. Вероятный ущерб от нарушений свойств безопасности определяется как низкий, так как удостоверяющий центр даже после нарушения сможет осуществлять свою деятельность. Таким образом информационная система получает третий класс защищенности, то есть для нее должна обеспечиваться нейтрализация угроз безопасности информации, связанных с действиями нарушителя с низким потенциалом. Совокупность мер защиты информации необходимых для этого перечислена в Приложении к Приказу и эквивалентна мерам, перечисленным в приложении к Приказу ФСТЭК от 18.02.2013 г. № 21. Однако имеются и дополнительные требования. Согласно этим требованиям в информационной системе необходимо будет применять:

- Средства вычислительной техники не ниже 5 класса;
- Системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- Межсетевые экраны не ниже 3 класса.

Обеспечиваемый при этом уровень безопасности информационной системы выходит не ниже, чем у системы третьего уровня защищенности по классификации Постановления Правительства РФ от 01.11.2012 № 1119.

Таким образом, информационная система, обеспечивающей электронный документооборот между удостоверяющим центром и его клиентами позволит значительно ускорить процесс оказания услуги по выпуску электронной подписи, сократив время на создание и проверку документов. При этом необходимо обеспечить безопасность персональных данных, обрабатываемых в данной информационной системе.

Библиографический список

1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

3. Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. №1119.

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

5. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Харечкин П.В.

Исследование угроз информационной безопасности робототехническим комплексам

В последние годы наблюдаются высокие темпы технологического развития, и одним из передовых направлений является робототехника, имеющая очень широкую область применения. При таком разнообразном использовании робототехнических устройств и систем возникает вопрос обеспечения безопасности их управления.

Основными параметрами защищенности для робототехнических комплексов (РТК), как и для любого объекта защиты, являются целостность, доступность и конфиденциальность [1]. При этом основное влияние на безопасность РТК оказывают два фактора: потенциальные возможности нарушителей информационной безопасности (ИБ) и порождаемые ими угрозы безопасности информации. Оптимальная система защиты информации может быть создана только по результатам оценки угроз ИБ РТК.

Анализ обобщенной модели ИБ РТК [2] позволяет провести теоретические исследования основных угроз ИБ РТК, а именно угроз несанкционированного доступа к информации ограниченного доступа, обрабатываемой в РТК (угроз непосредственного доступа в программную среду, угроз,