УДК 004.054

А.С. Марковский[1]
А.В. Самонов[2]
А.П. Киреев[6]

МЕТОДИКА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ РЕСУРСОВ ИНФРАСТРУКТУРЫ ЕДИНОГО ПРОСТРАНСТВА ДОВЕРИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

В статье описана методика оценки уровня защищенности ресурсов инфраструктуры единого пространства доверия электронной подписи (ЕПД-ЭП), предназначенная для обоснованного принятия решения по составу и характеристикам комплекса средств его защиты от случайных и преднамеренных угроз. В соответствии с методологией управления рисками идентифицированы основные активы инфраструктуры ЕПД-ЭП и определены актуальные для них угрозы безопасности. Предложены методы оценки безопасного функционирования ЕПД-ЭП в случае реализации соответствующих угроз.

Ключевые слова: *информационная безопасность, риск, уровень защищённости.*

A.S. Markovsky
A.V. Samonov
A.P. Kireev

THE UNITED SPACE OF DIGITAL SIGNATURE TRUST: A VALUATION METHOD OF ITS INFORMATION RESOURCES SECURITY

In the article the valuation method of information security of infrastructure resources of united trust space of a digital signature is submitted. The method is intended for the reasonable decision-making about structure and performance attributes of security features from accidental and premeditated threats. This method is based on the risk assessment methodology. This method allows to evaluate the assets, threats and degree of information security. The valuation methods of safe functioning of trust united space of a digital signature, in case of implementation of the relevant threats are offered.

Keywords*: information security, risk, security level/*

В рамках реализуемой в настоящее время государственной программы «Информационное общество (2011–2020 гг.)» в РФ осуществляются работы по развитию и модернизации целого ряда информационных систем, образующих инфраструктуру единого пространства доверия (ИЕПД) [1]. К ним относятся ЕПГУ (Единый портал государственных услуг), СМЭВ (система межведомственного электронного взаимодействия), ЕПД-ЭП (единое пространство доверия электронной подписи), ЕСИА (единая система идентификации и аутентификации) и другие. Корректное функционирование этих систем и обеспечение необходимого уровня доверия реализуемым с их помощью услуг в значительной степени будет определяться защищенностью соответствующих информационных, программных и коммуникационных ресурсов и средств.

В соответствии с [2], для обеспечения безопасности и надежного функционирования ЕПД должен быть осуществлен комплекс мероприятий, включающий организационные, правовые и технические меры по защите от несанкционированного доступа ко всем ресурсам ЕПД, непрерывную защиту от вредоносных программ и процессов, а также оперативное реагирование на инциденты информационной безопасности.

Современные технологии обеспечения безопасности информационных систем основаны на процессном подходе, который предполагает

[1] Кандидат технических наук, начальник лаборатории, старший научный сотрудник, Военно-космическая академия им. А.Ф. Можайского.

[2] Кандидат технических наук, ведущий научный сотрудник, Военно-космическая академия им. А.Ф. Можайского.

[3] Старший научный сотрудник, Военно-космическая академия им. А.Ф. Можайского.

осуществление систематически повторяющегося цикла процессов планирования, внедрения, проверки и улучшения СОИБ. Данные процессы реализуются посредством процедур управления рисками, управления ресурсами, управления инцидентами и модернизации [3; 4], схематично представленными на рис. 1.

Создание СОИБ начинается с этапа планирования, на котором осуществляется оценка уровня угроз безопасности для защищаемых ресурсов и определяется состав, характеристики и способы применения мер и средств защиты, способных противостоять этим угрозам.

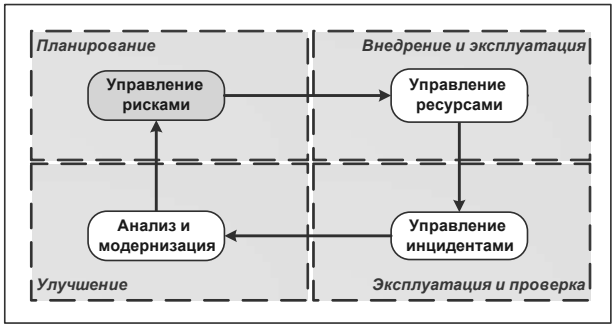

Рис. 1. Этапы и процедуры создания СОИБ

В данной статье описана методика реализации этого этапа построения СОИБ для ЕПД-ЭП, построенного на основе технологии открытых ключей.

Управление рисками – это процесс идентификации, оценивания, устранения или уменьшения вероятности событий, которые могут нанести ущерб защищаемым ресурсам (активам). Цель процедуры управления рисками состоит в том, чтобы уменьшить риски до приемлемого уровня. Процедура управления рисками в соответствии с [5] состоит в последовательном решении следующих пяти задач:

1) идентификация и оценка критичности защищаемых активов;

2) определение целей и возможностей потенциальных нарушителей;

3) идентификация и оценка вероятности реализации угроз, исходящих от потенциальных нарушителей с учетом имеющихся средств защиты;

4) оценка потенциального ущерба в случае реализации угроз с учетом имеющихся средств защиты;

5) принятие решения о допустимости рассчитанного ущерба (величины рисков) или формирование предложений по усилению системы защиты до состояния, обеспечивающего допустимый уровень риска.

Как показал проведенный анализ, в инфраструктуре ЕПД-ЭП можно выделить три группы активов:

1) информационные ресурсы, к которым относятся создаваемые и используемые для функционирования ЕПД-ЭП документы, данные и средства: закрытые ключи ЭП уполномоченных лиц УЦ (удостоверяющего центра), ключевая и аутентифицирующая информация субъектов УЦ, содержимое реестра сертификатов, электронные документы, подписанные ЭП, документация, программные и аппаратные средства УЦ и клиентов и др.;

2) сервисы, предоставляемые клиентам и пользователям ЕПД-ЭП: генерация ключей, выпуск сертификата, датирование ЭП, аннулирование сертификата, предоставление информации о статусе сертификата и др.;

3) службы, обеспечивающие функционирование инфраструктуры открытых ключей: аутентификация пользователей, контроль доступа, аудит и др.

Оценки критичности активов ЕПД-ЭП следует определять не для активов непосредственно, а для их свойств защищенности. Как известно, основными свойствами безопасности являются: конфиденциальность, целостность, доступность защищаемых информационных ресурсов, а также аутентичность, неотказываемость, подконтрольность осуществляемых над ними операций. Причиной нарушения свойств защищенности актива является реализация против него определенной угрозы.

Известно, что угрозы характеризуются следующими атрибутами: источником, уязвимостью, методом реализации, результатом. Источниками угроз могут быть люди, программы, оборудование, окружающая среда. Угрозы обычно реализуются посредством использования уязвимостей атакуемой системы. Примерами методов реализации угроз являются: внедрение программных и аппаратных закладок, атака на отказ в обслуживании, несанкционированный перехват и прослушивание сетевого трафика, установка вирусов и троянов и др. Основными типами результатов реализации угроз являются: нарушение перечисленных выше свойств защищенности: конфиденциальности, целостности, доступности, нарушение аутентичности, отказ от авторства и др. [6; 7; 8].

Оценкой (уровнем) критичности актива ЕПД-ЭП является условная вероятность нарушения безопасного функционирования ЕПД-ЭП по причине реализации против данного актива

определенной угрозы. Введем следующие обозначения:

$A = \{a_j\}$ – множество активов ЕПД-ЭП;

$B = \{b_i\}$ – множество угроз безопасности;

$P_{bi,aj}(S_{нр})$ – условная вероятность события, соответствующего нарушению работоспособности ЕПД-ЭП (переходу его в неработоспособное состояние – $S_{нр}$) по причине реализации против актива a_j угрозы b_i.

Оценки критичности активов в этом случае удобно представлять в табличном виде, например, как это представлено в таблице 1.

Таблица 1

Оценки критичности активов ЕПД-ЭП

Актив ЕПД	$P_{bi,aj}(S_{нр})$ – оценка критичности угрозы b_i для актива a_j			
	b_1	b_2	...	b_n
a_1	P_{11}	P_{12}	...	P_{1n}
a_2	P_{21}	P_{22}	...	P_{2n}
a_3	P_{31}	P_{32}	...	P_{3n}
...				
a_m	P_{m1}	P_{m2}	...	P_{mn}

Вероятность нарушения работоспособности ЕПД-ЭП по причине реализации против одного из его активов a_j угрозы b_i может быть рассчитана по следующей формуле:

$$P\left(S_{нр} / b_i > a_j\right) = P_{b_i,a_{ij}}\left(S_{нр}\right) \cdot P\left(b_i, a_j\right),$$

где $P\left(b_i, a_j\right)$ – вероятность успешной реализации угрозы b_i против актива a_j.

Для расчета вероятности нарушения функционирования ЕПД-ЭП в случае реализации нескольких угроз можно воспользоваться следующей формулой:

$$P\left(S_{нр} / B > A\right) = 1 - \Pi\left(Q\left(S_{нр} / b_i > a_j\right)\right),$$

где $Q\left(S_{нр} / b_i > a_j\right) = 1 - P\left(S_{нр} / b_i > a_j\right)$ – вероятность противоположного события;

$\Pi\left(Q\left(S_{нр} / b_i > a_j\right)\right)$ – произведение вероятностей.

Наиболее опасными для ЕПД-ЭП являются угрозы, направленные на нарушение корректного функционирования его основных сервисов. На рис. 2 представлена обзорная диаграмма взаимодействия пользователей и компонентов инфраструктуры ЕПД-ЭП при информационном обмене. Компоненты инфраструктуры ЕПД-ЭП изображены в виде шести серверов: регистрации, сертификации, каталогов, датирования, восстановления ключей и ведения архива, каждый из которых реализует определенный набор сервисов.

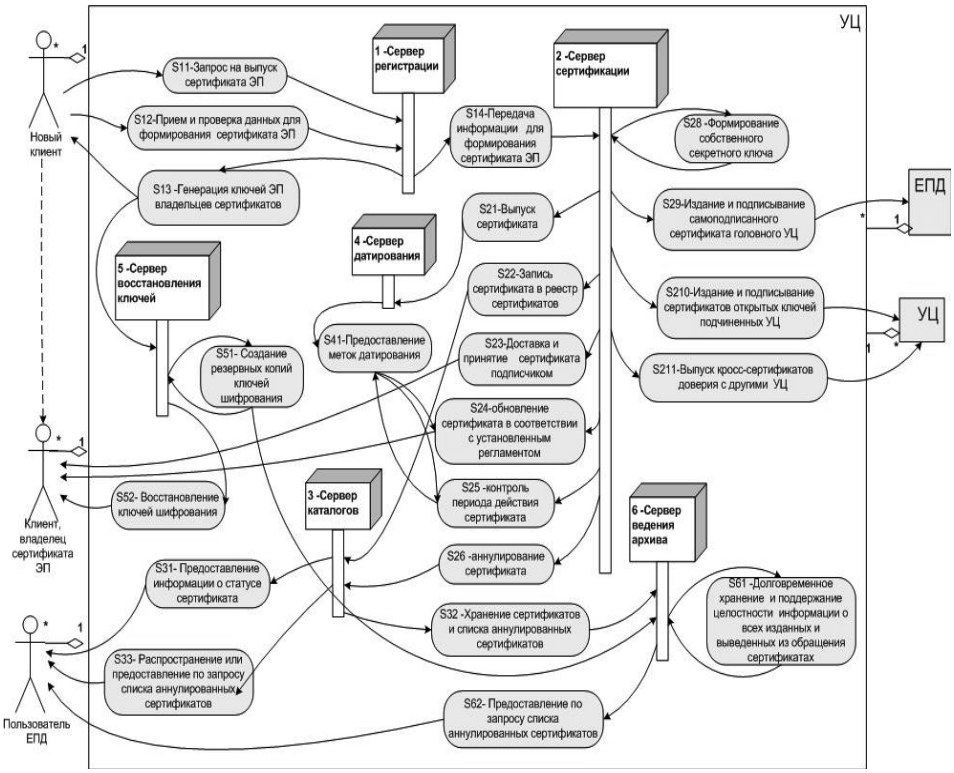

Рис. 2. Обзорная диаграмма взаимодействия основных компонентов ЕПД-ЭП

Процедуру оценивания критичности отдельных сервисов для безопасности функционирования ЕПД-ЭП рассмотрим на примере сервера регистрации. Как видно из рис. 2, его основными функциями являются:

1) s_{11} – прием от клиентов запросов на выпуск сертификатов;

2) s_{12} – прием и проверка идентификационных и других необходимых для формирования сертификата ЭП данных;

3) s_{13} – генерация ключей ЭП владельцев сертификатов;

4) s_{14} – передача в УЦ информации, необходимой для формирования сертификата ЭП.

Основными угрозами для безопасного и корректного функционирования сервера регистрации являются нарушения доступности – r_d, аутентичности – r_a, достоверности – r_t, неотказываемости – r_n и подконтрольности – r_k выполнения приведенных выше функций. В случае успешной реализации этих угроз возможны следующие негативные последствия:

1) в случае нарушения аутентичности и достоверности функций s_{12} и s_{14} возможно получение и использование в сертификате открытого ключа ЭП недостоверных (фальсифицированных) идентификационных данных;

2) в случае нарушения аутентичности и достоверности функции s_{13} возможно создание нестойких ключей ЭП посредством использования уязвимостей средств генерации ключей и несанкционированного доступа к серверу регистрации;

3) в случае нарушения аутентичности и достоверности функций s_{12} и s_{14} возможны фальсификация, перехват и компрометация сгенерированных ключей ЭП и идентификационных данных.

Для ЕПД-ЭП при этом возникают следующие риски:

1) распространение документов с ЭП от имени другого лица или организации;

2) возможность фальсификации (подделки) ЭП владельца скомпрометированного ключа;

3) возможность использовать чужую ЭП;

4) досрочное прекращение возможности использования ЭП или использование ключей ЭП, срок действия которых истек и сертификат на которые стал недействителен.

В таблице 2 представлен пример оценок критичности для ЕПД-ЭП-операций, выполняемых сервером регистрации. Значения этих оценок выражены в форме условных вероятностей нарушения функционирования ЕПД-ЭП в случае реализации угроз, приводящих к нарушению свойств достоверности, аутентичности, доступности, подконтрольности и неотказуемости выполнения соответствующих операций (сервисов).

Таблица 2

Оценки критичности нарушений функционирования сервисов, выполняемых сервером регистрации, для надежной и безопасной работы ЕПД-ЭП

Сервис/операция	Оценка критичности для безопасности функционирования ЕПД-ЭП-сервисов, выполняемых сервером регистрации				
	r_t	r_d	r_a	r_k	r_n
s_{11}	0	1	1	0,7	0,7
s_{12}	1	1	1	0,8	0,8
s_{13}	1	1	1	0,9	0,9
s_{14}	1	1	1	0,9	0,9

Основными способами реализации атак на компоненты ЕПД-ЭП являются [9; 10]:

– m_1 – подбор или взлом паролей;

– m_2 – несанкционированный доступ в обход средств защиты;

– m_3 – истощение ресурсов;

– m_4 – злоупотребление функциональностью;

– m_5 – повышение привилегий;

– m_6 – внедрение программных и аппаратных закладок в технические и программные средства;

– m_7 – использование вирусов, троянов и другого зловредного программного обеспечения (ПО);

– m_8 – маскарад (злоумышленник посылает электронный документ (ЭД) от имени легального пользователя ЕПД-ЭП);

– m_9 – переделка (злоумышленник посылает измененный ЭД от имени легального пользователя ЕПД-ЭП);

– m_{10} – фальсификация меток времени и даты подписания ЭД;

– m_{11} – компрометация закрытого ключа ЭП;

– m_{12} – фальсификация содержимого сертификата открытого ключа.

В соответствии с методологией управления рисками для каждого актива $\boldsymbol{a}_i$ и риска $\boldsymbol{R}_j$ необходимо:

– определить способ реализации угрозы (m_k) и оценить ее потенциал $p(u_i)$;

– определить способ защиты (z_n) и оценить потенциал этой защиты в отношении конкретной угрозы $p(z_n)$;

– оценить остаточный риск $dR(u_i, z_n)$.

Необходимые для решения этой задачи данные могут быть представлены в табличном виде (таблица 3).

Таблица 3

Оценки рисков ЕПД-ЭП в случае реализации угроз безопасности

Угроза $u_i(b_i > a_j \mid h_l m_k)$	Потенциал угрозы u_i	Средство защиты z_i	Потенциал защиты (степень противодействия угрозе) $p(z_i)$	Остаточный риск $dR(u_i, z_i)$
$u_1(b_1 > a_1 \mid h_1 m_1)$	$p(u_1)$	z_1	$p(z_1)$	$dR(u_1, z_1)$
$u_2(b_2 > a_1 \mid h_1 m_1)$	$p(u_2)$	z_2	$p(z_2)$	$dR(u_2, z_2)$
…	…	…	…	…
$u_n(b_n > a_n \mid h_n m_n)$	$p(u_n)$	z_n	$p(z_n)$	$dR(u_n, z_n)$

Для нейтрализации определенной угрозы могут использоваться несколько средств защиты. В этом случае их потенциал будет суммироваться. Ниже представлен перечень основных мер и средств защиты, которые рекомендуется использовать для обеспечения безопасного функционирования ЕПД-ЭП.

1. Применение сертифицированных аппаратных и программных средств.
2. Применение межсетевого экранирования.
3. Аутентификация абонентов и шифрование передаваемой защищаемой информации.
4. Аутентификация абонентов, обеспечение целостности посредством использования механизма ЭП.
5. Использование средств 2-факторной аутентификации.
6. Контроль доступа.
7. Использование средств защиты от атак на отказ в обслуживании.
8. Дублирование и резервирование, использование отказоустойчивых систем.
9. Антивирусная защита.
10. Регулярное тестирование сканерами безопасности и устранение обнаруженных уязвимостей.
11. Применение сертифицированных систем обнаружения атак.
12. Физическая защита помещений, аппаратных и программных средств.

Остаточный риск может быть рассчитан по формуле:

$$dR(u_n, z_n) = p(u_n) - p(z_n).$$

В случае если остаточный риск не превышает некоторого допустимого значения $dR(u_n, z_n) \le dR^{доп}$, то считается, что система защищена от данной угрозы. В противном случае необходимо в систему защиты включить дополнительные меры и/или средства, которые бы свели остаточный риск до приемлемого.

В таблице 4 приведены примеры оценки рисков безопасности ЕПД-ЭП в случае реализации атак на ряд информационных ресурсов ЕПД-ЭП.

В первой строке таблицы представлены оценки рисков ЕПД-ЭП при реализации угроз безопасности b_1 – нарушение конфиденциальности актива a_1 – закрытый ключ ЭП УЦ. Данную угрозу реализует нарушитель h_2 – хакер, использующий канал общей сети доступа с помощью метода m_1 – подбор или взлом ключа ЭП УЦ. В качестве мер и средств защиты используются: z_1 – применение сертифицированного ПО и z_3 – межсетевое экранирование сервера УЦ. Остаточный риск dR_1 – «компрометация ключа ЭП УЦ» – сведен к нулю.

Таблица 4

Примеры оценок рисков ЕПД-ЭП при реализации угроз безопасности

Угрозы	Потенциал угрозы	Меры и средства защиты	Потенциал защиты	Остаточный риск
$u_1(b_1 > a_1 \mid h_2 m_1)$	0,7	$z_1 z_3$	0,7	0
$u_2(b_2 > a_2 \mid h_2 m_2)$	0,8	$z_1 z_5$	0,75	0,05
$u_3(b_2 > a_3 \mid h_3 m_6)$	1,0	$z_1 z_3 z_5$	0,6	0,4

Во второй строке представлены оценки рисков ЕПД-ЭП при реализации угроз безопасности b_1 – нарушение конфиденциальности актива a_2 – ключевая и аутентифицирующая информация субъектов УЦ. Данную угрозу реализует нарушитель h_2 – хакер, использующий канал общей сети доступа с помощью метода m_2 – несанкционированный доступ в обход средств защиты.

В качестве мер и средств защиты используются: z_1 – использование сертифицированного ПО и z_5 – использование средств 2-факторной аутентификации. Остаточный риск dR_2 – «компрометация ключа ЭП УЦ» – равен 0,05 и может считаться допустимым.

В третьей строке представлены оценки рисков ЕПД-ЭП при реализации угроз безопасности b_2 – нарушение целостности актива a_3 – сертификат подчиненного УЦ. Данную угрозу реализует нарушитель h_3 – субъекты,

входящие в организованные корпоративные и государственные структуры и организации, с помощью метода m_6 – внедрение программных и аппаратных закладок в технические и программные средства. В качестве мер и средств защиты используются: z_1 – использование сертифицированного ПО, z_3 – межсетевое экранирование сервера УЦ и z_5 – использование средств 2-факторной аутентификации. Остаточный риск dR_2 – «компрометация сертификата подчиненного УЦ» – равен – 0,4. Такой риск не может считаться допустимым, поэтому необходимо усиливать систему защиты.

Заключение. Предложенная методика оценки уровня угроз безопасности ресурсов инфраструктуры ЕПД-ЭП, реализуемая в целях определения необходимого и достаточного комплекса средств защиты, представляет научный и практический интерес. Применение и развитие методики позволит проводить исследования безопасности, анализ рисков и определять требования к составу и характеристикам СОИБ ЕПД-ЭП.

Литература

1. Государственная программа Российской Федерации «Информационное общество (2011–2020 годы». Утвер. Распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-Р [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html свободный, дата проверки: 21.11.2015 г.

2. Системный проект формирования в Российской Федерации инфраструктуры электронного правительства [Электронный ресурс]. – Режим доступа: https://smev.gosuslugi.ru/portal/api/files/get/652 свободный, дата проверки: 21.11.2015 г.

3. Международный стандарт ISO/IEC FDIS 17799:2005 (ISO 27002:2007). Информационные технологии. Методики безопасности. Практические правила управления информационной безопасностью.

4. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

5. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий.

6. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» [Электронный ресурс]. – Режим доступа свободный: http://d-russia.ru/wp-content/uploads/2015/05/metodic.pdf., дата проверки: 21.11.2015 г.

7. Сабанов А.Г. Методика анализа рисков аутентификации при удалённом электронном взаимодействии. Докл. на XVI Междунар. конф. «Рускрипто-2014». Интернет-ресурс:http://www.ruscrypto.ru/accotiation/archive/rc2014/.

8. ГОСТ Р ИСО 31010-2011. Менеджмент риска. Методы оценки риска [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-31010-2011, дата проверки: 21.11.2015 г.

9. Common Weakness Enumeration (CWE) [Электронный ресурс]. – Режим доступа: http://cwe.mitre.org/. свободный, дата проверки: 21.11.2015 г.

10. Common Attack Pattern Enumeration and Classification (CAPEC) / [Электронный ресурс]. – Режим доступа: http://capec.mitre.org/. свободный, дата проверки: 21.11.2015 г.

11. Нечай А.А. Методика комплексной защиты данных, передаваемых и хранимых на различных носителях / А.А. Нечай, П.Е. Котиков // Вестник Российского нового университета.Серия «Сложные системы: модели, анализ и управление». – 2015. – Выпуск 1. – С. 92–95.