УДК 004.056

М.Л. Соловьев, Т.Е. Минеева, А.А. Конев, Д.Н. Буинцев

Модель угроз безопасности, возникающих при управлении системой защиты информации

Представлена модель угроз, направленная на повышение уровня безопасности системы защиты информации. Для построения модели используется теория графов и теория управления бизнес-процессами. Разработанная модель включает угрозы, направленные на кадровый, технический и нормативный компоненты системы защиты информации. Типы угроз сформированы на основе цикла Деминга, что позволяет учесть все значимые процессы управления системой. Учёт всех значимых компонентов и процессов управления системой защиты информации является существенным преимуществом по сравнению с существующими моделями угроз.
Ключевые слова: модель угроз безопасности, система защиты информации, угрозы целостности, жизненный цикл, процессы управления, перечень угроз информации.
doi: 10.21293/1818-0442-2019-22-3-31-36

На сегодняшний день очень важным вопросом является обеспечение безопасности системы защиты информации в целом. Так как в основном внимание уделяют защите информации, носителям информации, средствам защиты, находящимся в организации, а регламентирующей документации не хватает должного внимания, что и является угрозой процессам управления системы защиты информации (СЗИ).

В существующих приказах и нормативных документах не прописано, что угрозы, направленные на процессы управления, должны рассматриваться на всех этапах ее жизненного цикла, а именно, рассмотрев угрозы на каждом этапе, безопасность управленческих процессов системы защиты информации станет эффективнее и максимально надежнее. Поэтому регламентация управленческих процессов очень важна, так как через нее и осуществляется управление системой защиты информации в целом.

Согласно приказу ФСТЭК №235 [1] и ГОСТу Р 50922–2006 [2], система защиты информации является совокупностью персонала, технических средств обеспечения безопасности, а также правил и норм, установленных соответствующими документами в области защиты информации. Таким образом, модель угроз должна включать все три составляющие системы защиты информации.

Общий подход к структуре модели угроз приведен в [3] и включает следующие классы угроз:

– перечень угроз, направленных на информацию и ее носители;

– перечень угроз, направленных на элементы информационной системы и системы защиты;

– перечень угроз, направленных на процессы управления системой защиты.

В работе [4] рассматриваются модели классификации угроз, аргументируется отсутствие полноты в существующих моделях классификации угроз, также предлагается использовать смешанную модель классификации угроз, которая позволяет определять характеристики данных угроз.

В работах [5–8] предложены методики оценки рисков и выявления актуальных угроз безопасности исследуемой информационной системы, разработанные на основе моделей угроз безопасности.

У существующих моделей угроз безопасности отсутствует необходимый перечень угроз, что является существенным недостатком, так как в дальнейшем невозможно будет сформировать обоснованные требования к обеспечению безопасности процессов управления СЗИ. Кроме того, угрозы, направленные на нарушение процессов управления системой, практически отсутствуют, и они не структурированы, что не позволяет составить максимально полный перечень угроз.

Подходы к построению моделей угроз, направленные на информационные системы, а также информацию и ее носители, описаны в [9, 10]. В этих же работах представлены модели самих объектов защиты – информационных систем и информационных потоков, реализованных в данных системах. Таким образом, дополнительно к этим моделям угроз необходимо разработать модели объекта защиты и угроз с точки зрения управления информационной системой.

Модель жизненного цикла системы защиты

Модель жизненного цикла системы защиты основана на классификации процессов управления системой и ее компонентами. В качестве классов взяты элементы системы защиты – персонал, программно-аппаратные средства обеспечения безопасности и организационная документация, в соответствии с которой функционирует система безопасности [11].

Перечень этапов жизненного цикла основывается на определении состояний и переходов между ними системы защиты информации и/или ее компонентов (работоспособность, выход из строя, потеря актуальности и т.п.) [12]. Учитываемые этапы жизненного цикла:

– приобретение (разработка) компонента системы защиты и вывод элемента из системы;

– ввод в эксплуатацию элемента системы защиты и вывод компонента из эксплуатации;

– эксплуатация компонента системы защиты;

– контроль актуальности компонента системы защиты и его обновление;

– контроль функционирования компонента системы защиты и его восстановление.

Процессы, связанные с вводом/выводом из эксплуатации, подразумевают включение/исключение компонента из системы защиты. Например, применительно к персоналу – это предоставление прав доступа к защищаемой информации сотрудника или отзыв прав на работу с данной информацией.

Предложенные этапы жизненного цикла могут быть представлены следующим образом [13]:

– планирование;

– ввод в эксплуатацию;

– эксплуатация;

– контроль за функционированием;

– улучшение;

– вывод из эксплуатации;

– уничтожение.

Предложенная классификация позволила формализовать модели жизненного цикла программно-аппаратных средств защиты, персонала организации, а также нормативной документации [14].

На основе моделей жизненного цикла составляющих системы защиты информации была составлена типовая модель жизненного цикла самой системы защиты информации (рис. 1).

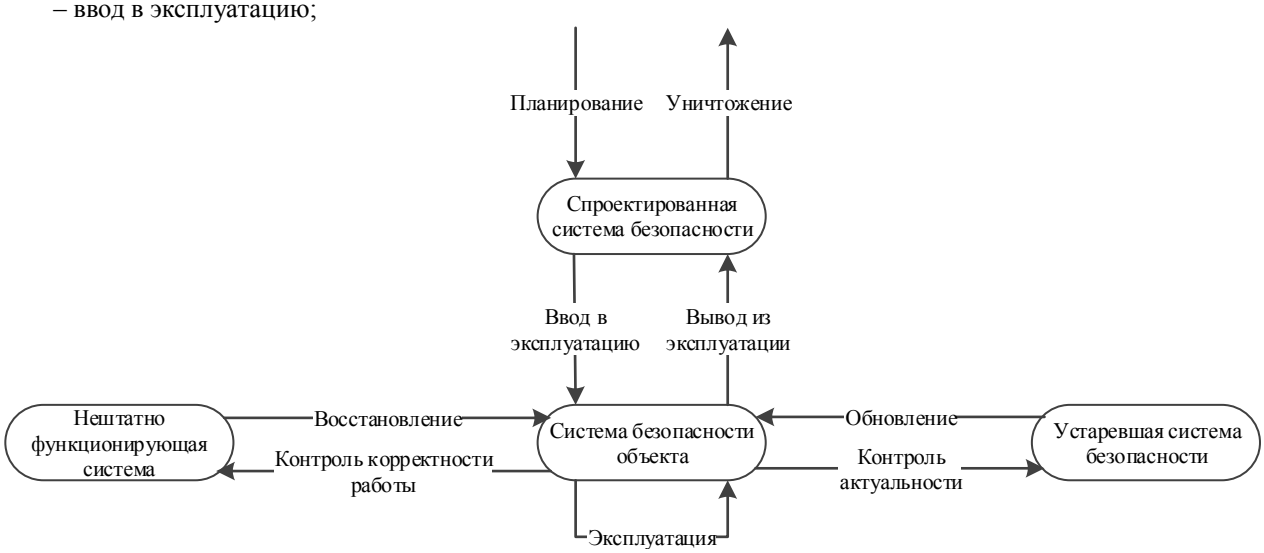

Рис. 1. Модель жизненного цикла системы защиты информации

Модель жизненного цикла системы защиты информации отражает состояния и процессы управления ее составляющих, а именно программно-аппаратных средств защиты, нормативной документации и персонала, также при ее построении были учтены основные этапы жизненного цикла системы.

Данная модель позволит рассмотреть каждый из классов процессов управления более подробно и раскрыть перечень угроз, направленных непосредственно на состояние системы защиты в процессе ее управления. Соответственно, рассмотрев перечень угроз, можно будет описать механизмы защиты, направленные на минимизацию этих угроз, что обеспечит безопасность работы системы защиты информации.

Модель угроз

Управление системой защиты информации подразумевает регламентацию этапов жизненного цикла за счет составления организационной документации. Под «организационной документацией» в данном случае подразумевается не документ, а правила, в нем зафиксированные. Таким образом, типовые угрозы направлены на процессы управления компонентами системы защиты информации (программно-аппаратными средствами, нормативной документацией и персоналом) с точки зрения некорректной разработки или применения этих правил. Подход к рассмотрению угроз управления СЗИ основан на цикле Деминга, так как данный постоянный круг действий направлен на усовершенствование и улучшение процессов [15]. Цикл Деминга представляет алгоритм действий, состоящий из следующих стадий:

– проектирование;

– выполнение;

– контроле;

– корректировка.

На каждом этапе цикла были рассмотрены соответствующие угрозы управляющим процессам СЗИ и выделены типовые угрозы (таблица).

Нейтрализация данных типов угроз направлена на понимание требований безопасности управленческих процессов, необходимости внедрения и использования мер безопасности, непрерывный контроль и мониторинг производительности и эффективности управления СЗИ, а также ее улучшение [16].

При составлении перечня угроз были учтены все существующие процессы каждого этапа жизненного цикла системы защиты информации. Например, для персонала представлены следующие процессы управления:

– прием на работу;

– допуск к конфиденциальной информации;

– выполнение своих обязанностей;

– идентификация текущего состояния статуса сотрудника;

– повышение квалификации;

– контроль корректности работы;

– восстановление качества выполняемых обязанностей сотрудника;

– лишение прав на работу с конфиденциальной информацией;

– увольнение.

Типовые угрозы, возникающие на этапах жизненного цикла СЗИ

Угрозы	
Целостности	Конфиденциальности
Некорректная разработка регламента процесса	Разглашение информации об особенностях разработки регламента процесса
Некорректное исполнение регламента процесса	Разглашение правил работы, указанных в регламенте
Некорректная организация контроля за исполнением регламента процесса	Разглашение информации о принципах организации контроля за исполнением регламента процесса
Неполная корректировка возможных ошибок, найденных в регламенте процесса	Разглашение информации об обнаруженных ошибках, найденных в регламенте процесса, и правил их корректировки

Таким образом, были рассмотрены процессы управления для нормативной документации и программно-аппаратного обеспечения. Каждый процесс управления регламентируется управляющими документами, перечень которых был тоже подобран и рассмотрен для более детального описания угроз, направленных на процессы управления системой защиты.

Для наглядного отображения модели угроз безопасности используется теория графов, а именно, неориентированный граф, отражающий соответствие угроз безопасности процессам управления системой защиты, на которые данные угрозы направлены.

Множество типовых угроз было обозначено, как

$$U = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8\},$$

где u_1 – угроза некорректной разработки регламента процесса; u_2 – угроза некорректного исполнения регламента процесса; u_3 – угроза некорректной организации контроля за исполнением регламента процесса; u_4 – угроза неполной корректировки возможных ошибок, найденных в регламенте процесса; u_5 – угроза разглашения информации об особенностях разработки регламента процесса; u_6 – угроза разглашения правил работы, указанных в регламенте; u_7 – угроза разглашения информации о принципах организации контроля за исполнением регламента процесса; u_8 – угроза разглашения информации об обнаруженных ошибках, найденных в регламенте процесса, и правил их корректировки.

Множество процессов управления обозначено как

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9\},$$

где v_1 – процессы, связанные с планированием (разработкой или подбором компонента); v_2 – процессы, связанные с вводом компонента в эксплуатацию; v_3 – процессы, связанные с эксплуатацией компонента; v_4 – процессы, связанные с контролем актуальности компонента; v_5 – процессы, связанные с обновлением компонента; v_6 – процессы, связанные с контролем функционирования компонента; v_7 – процессы, связанные с восстановлением компонента; v_8 – процессы, связанные с выводом компонента из эксплуатации; v_9 – процессы, связанные с исключением компонента из системы.

Множество компонентов системы защиты информации обозначено как

$$M = \{m_1, m_2, m_3\},$$

где m_1 – программно-аппаратные средства защиты; m_2 – нормативная документация; m_3 – персонал.

На множествах U и V введем отношение «существует», выделив в декартовом произведении множеств $U \times V$ подмножество упорядоченных пар, обладающих свойством: множество угроз U_i существует на множестве процессов управления V_j.

Бинарное отношение было обозначено $\alpha \subset U \times V$

$$\alpha = \{(U_i^{mk}, V_i^{mk})\},$$

где $i = 1…6$ – номер типа угрозы, $j = 1…9$ – номер процесса управления, k – номер элемента системы защиты информации.

Результатом данного отношения α будет являться полный перечень угроз, существующих на каждом из процессов управления системой защиты информации.

Например, отношение $\alpha = \{(U_5^{m3}, V_4^{m3})\}$ будет означать, что для такого элемента СЗИ, как персонал, на этапе контроля актуальности выполняемых обязанностей существует угроза разглашения информации о некорректном планировании инструкции, регламентирующей процесс контроля актуальности выполняемых обязанностей сотрудника. Данная угроза является угрозой конфиденциальности процесса контроля актуальности и влияет на стабильность функционирования данного процесса тем, что такая информация может нанести ущерб организации со стороны злоумышленника.

А отношение $\alpha = \{(U_2^{m1}, V_9^{m1})\}$ означает, что для программного обеспечения на этапе его удаления существует угроза неверного обучения инструкции, регламентирующей процесс удаления исполнителем данного процесса. Данная угроза является угрозой целостности для процесса удаления программного обеспечения, так как исполнитель, который плохо обучен регламенту, нарушает целостность процесса удаления.

Собственно моделью угроз и будет считаться полное соответствие существующих угроз управляющим процессам (рис. 2). В данной модели учитываются все угрозы, которые направлены на регламентирующую документацию на каждом этапе ее совершенствования, а именно на этапе планирования, на этапе обучения персонала, на этапе поиска ошибок и на этапе исправления найденных ошибок, содержащихся в регламентирующей документации процессов управления системой защиты информации.

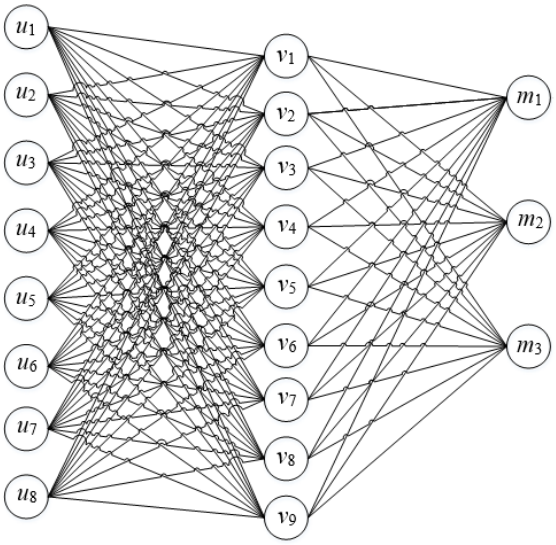

Рис. 2. Модель угроз безопасности, направленных на процессы управления СЗИ

Данная модель обладает полнотой угроз, относящихся к каждому классу процессов управления. Каждому типу угроз соответствует этап жизненного цикла, на котором она реализуется, а этап жизненного цикла, в свою очередь, соответствует определенному компоненту СЗИ. Использование данной модели позволит получить максимально возможный перечень угроз, что позволит повысить уровень защищенности системы защиты в целом и ее отдельных компонентов.

Перечень угроз составлен для каждого компонента СЗИ и всех предложенных процессов управления на основе модели жизненного цикла системы защиты информации. Стоит отметить, что подобные угрозы не включены в банк угроз ФСТЭК, что еще раз доказывает актуальность данной проблемы и необходимость рассмотрения данного вопроса.

Актуальность данной модели можно обосновать сравнением со следующими нормативными документами в области информационной безопасности:

– приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [17];

– приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ Федеральной службы по техническому и экспортному контролю»;

– приказ ФСТЭК России 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [18].

Сравнивая разработанную модель с требованиями по обеспечению безопасности и создания систем безопасности, можно отметить, что некоторые процессы управления, на которые направлены угрозы, рассматриваются и в данных требованиях. Но также модель угроз учитывает те процессы, которые в перечисленных нормативных актах не рассматриваются, например, лишение прав сотрудника на работу с конфиденциальной информацией и восстановление корректности работы элемента СЗИ.

Заключение

Разработанная модель, в отличие от аналогов, включает типы угроз для всех классов компонентов системы защиты информации, а также учитывает все типовые процессы управления, что является преимуществом перед существующими моделями угроз.

Все процессы управления, рассматриваемые в приказах ФСТЭК, учитываются в разработанной модели жизненного цикла СЗИ. Разработанная модель содержит расширенный перечень процессов управления и направленных на эти процессы угроз, по сравнению с банком угроз ФСТЭК. При этом предложенная модель включает в разрезе угроз набор требований по обеспечению безопасности объектов СЗИ.

Угрозы, направленные на процессы, регламентирующие работу СЗИ, рассматриваются на каждом этапе жизненного цикла системы, что не прописывается ни в одном нормативном документе по информационной безопасности. При составлении типовых угроз, направленных на процессы управления, был использован цикл Деминга, что при нейтрализации данных угроз значительно повлияет на усовершенствование и улучшение управления СЗИ. Построенная модель угроз наглядно показывает соответствие элемента СЗИ, процесса управления и угроз, направленных на них.

Работа выполнена при финансовой поддержке Министерства высшего образования и науки РФ в рамках базовой части государственного задания ТУСУРа на 2017–2019 гг. (проект № 2.8172.2017/8.9).

Литература

1. Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236, свободный (дата обращения: 20.07.2019).

2. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Введ. 2008-02-01. – М.: Стандартинформ, 2008. – 12 с.

3. Конев А.А. Подход к описанию структуры системы защиты информации / А.А. Конев, Е.М. Давыдова // Доклады ТУСУР. – 2013. – № 2 (28). – С. 107–111.

4. Jouini M. Classification of Security Threats in Information Systems / M. Jouini, L. Ben Arfa Rabai, A. Ben Aissa // Procedia Computer Science. – 2014. – Vol. 32. – P. 489–496.

5. Шувалов И.А. Математическая модель воздействия угроз на информационную систему обработки персональных данных / И.А. Шувалов, Е.А. Семенчин // Фундаментальные исследования. – 2013. – № 10-3. – С. 529–533.

6. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

7. Миронова В.Г. Анализ этапов предпроектного обследования информационной системы персональных данных / В.Г. Миронова, А.А. Шелупанов // Вестник Сиб. гос. аэрокосм. ун-та им. акад. М.Ф. Решетнева. – 2011. – № 2 (35). – С. 45–48.

8. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Изв. ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 39–45.

9. Novokhrestov A. Mathematical model of threats to information systems / A. Novokhrestov, A. Konev // Prospects of Fundamental Sciences Development, PFSD-2016. AIP Conf. Proc. 1772. – 060015.

10. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин // Вест. Иркут. гос. техн. ун-та. – 2017. – Т. 21, № 10. – С. 93–104.

11. Королева О.Ю. Модель и метод оценки эффективности системы обеспечения информационной безопасности корпоративного хранилища данных кредитных организаций Российской Федерации: дис. ... канд. техн. наук. – СПб., 2012. – 124 с.

12. ГОСТ Р ИСО/МЭК 15288–2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. – М.: Стандартинформ, 2006. – 53 с.

13. Базаров Т.Ю. Управление персоналом: учеб. для вузов / Т.Ю. Базаров, Б.Л. Еремин. – М.: Банки и биржи, ЮНИТИ, 1998. – 423 с.

14. Модель жизненного цикла системы защиты информации / А.А. Конев, Т.Е. Минеева, М.Л. Соловьёв, А.А. Шелупанов, М.П. Силич // Безопасность информационных технологий. – 2018. – Т. 25, № 4. – С. 34–41.

15. Адлер Ю.П. Методы постоянного совершенствования сквозь призму цикла Шухарта–Деминга / Ю.П. Адлер, Е.И. Хунузиди, В.Л. Шпер // Методы менеджмента качества. – 2005. – № 3. – С. 29–36.

16. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Введ. 2006-27-12. – М.: Стандартинформ, 2006. – 31 с.

17. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239, свободный (дата обращения: 20.07.2019).

18. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: приказ Федеральной службы по техническому и экспортному контролю от 22.12.2017 г. № 236 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236, свободный (дата обращения: 20.07.2019).

Соловьев Михаил Леонидович
И.о. ректора Сибирского гос. ун-та телекоммуникаций и информатики (СибГУТИ)
Кирова ул., д. 86, г. Новосибирск, Россия, 630102
ORCID 0000-0002-4242-5571
Тел.: +7 (383-2) 69-83-15
Эл. почта: miksol57@list.ru

Минеева Татьяна Евгеньевна
Выпускник каф. безопасности информационных систем (БИС) Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
ORCID 0000-0003-1702-8731
Тел.: +7 (382-2) 70-15-29
Эл. почта: tatianamineeva7@gmail.com

Конев Антон Александрович
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
ORCID 0000-0002-3222-9956
Тел.: +7 (382-2) 70-15-29
Эл. почта: kaa1@keva.tusur.ru

Буинцев Дмитрий Николаевич
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 90-01-01
Эл. почта: buintsev-dn@tusur.ru

Soloviev M.L., Mineeva T.E., Konev A.A., Buintsev D.N.

Model of security threats arising from the management of information security systems

This paper presents a threat model aimed at improving the security level of an information protection system. To build the model, graph theory and business process management theory are used. The developed model includes threats aimed at personnel, technical and regulatory components of the information protection system. The types of threats are formed on the basis of the Deming cycle, which allows to take into account all the significant processes of system management. Taking into account all the significant components and processes of managing the information security system is a significant advantage over existing threat models.

Keywords: security threat model, information protection system, integrity threats, life cycle, management processes, list of information threats.
doi: 10.21293/1818-0442-2019-22-3-31-36

References

1. *Ob utverzhdenii Trebovaniy k sozdaniyu system bezopasnosti znachimyh obyektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i obespecheniyu ih funktsionirovaniya* [On approval of the Requirements for the creation of security systems of significant objects of the critical information infrastructure of the Russian Federation and ensuring their functioning]: the order of the Federal Service for Technical and Export Control dated December 21, 2017, no. 235. (in Russ.). Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236 (accessed: July 20, 2019).

2. GOST R 50922–2006. *Zaschita informatsii. Osnovnyye terminy i opredeleniya* [GOST R 50922–2006. Protection of information. Basic terms and definitions]. M., 2008. 12 p. (in Russ.).

3. Konev A.A., Davydova E.M. [Approach to the description of the structure of the information security system]. *Proceedings of TUSUR University*, 2013, no. 2 (28), pp. 107–111 (in Russ.).

4. Jouini M., Ben Arfa Rabai L., Ben Aissa A. Classification of Security Threats in Information Systems. *Procedia Computer Science*, 2014, vol. 32, pp. 489–496.

5. Shuvalov I.A., Semenchin E.A. [Mathematical model of impact of threats on information system of processing of personal information]. *Fundamental research*, 2013, no. 10-3, pp. 529–533 (in Russ.).

6. Prischep, A.A., Timchenko S.V., Shelupanov A.A. [Approaches and criteria for assessing information security risks]. *IT Security (Russia)*, 2007, no. 4, pp. 15-21 (in Russ.).

7. Mironova V.G., Shelupanov A.A. [Analysis of stages preproject survey information system of personal data]. *Vestnik SibSAU*, 2011, no. 2 (35), pp. 45–48 (in Russ.).

8. Mironova V.G., Shelupanov A.A. [Methodology of formation of threats of safety confidential information in uncertain conditions of their emergence]. *Izvestiya SFedU. Engineering sciences*, 2012, no. 12 (137), pp. 39–45 (in Russ.).

9. Novokhrestov A., Konev A. Mathematical model of threats to information systems. *Prospects of Fundamental Sciences Development, PFSD-2016. AIP Conf. Proc.*, 1772, 060015.

10. Novokhrestov A.K., Konev A.A., Shelupanov A.A., Yegoshin N.S. [Information and information carrier security threat model]. *Proceedings of Irkutsk State Technical University*, 2017, vol. 21, no. 10, pp. 93–104 (in Russ.).

11. Koroleva O.Yu. *Model' i metod otsenki effektivnosti sistemy obespecheniya informatsionnoy bezopasnosti korporativnogo khranilishcha dannykh kreditnykh organizatsiy Rossiyskoy Federatsii* [A model and method for assessing the effectiveness of the information security system of a corporate data warehouse of credit institutions of the Russian Federation. Thesis of Cand. of Tech. Science.]. SPb., 2012, 124 p. (in Russ.).

12. GOST R ISO/IEC 15288-2005. *Informatsionnaya tehnologiya. Sistemnaya inzheneriya. Protsessy zhiznennogo tsikla sistem* [GOST R ISO/IEC 15288-2005. Information technology. System engineering. System life cycle processes]. M., 2006, 53 p. (in Russ.).

13. Bazarov T.Yu., Eremin B.L. *Upravlenie personalom* [Personnel Management]. M., Banks and stock exchanges, UNITI, 1998, 423 p. (in Russ.).

14. Konev, A.A., Mineeva T.E., Soloviev M.L., Shelupanov A.A., Silich M.P. [Model of the life cycle of the information security system]. *IT Security (Russia)*, 2018, vol. 25, no. 4, pp. 33–41 (in Russ.).

15. Adler Yu.P., Hunuzidi E.I., Shper V.L. [Methods of continuous improvement through the prism of the Shewhart-Deming cycle]. *Quality management methods*, 2005, no. 3, pp. 29–36 (in Russ.).

16. GOST R ISO/IEC 27001-2006. Informatsionnaya tehnologiya. Metody I sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti [GOST R ISO/IEC 27001-2006. Information technology. Methods and means of security. Information security management systems]. M., 2006, 31 p. (in Russ.).

17. *Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimyh obyektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii* [On the approval of the Requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation]: the order of the Federal Service for Technical and Export Control dated 25.12.2017, no. 239 (in Russ.). Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed: July 20, 2019).

18. *Ob utverzhdenii formy napravleniya svedeniy o rezultatah prisvoeniya obyektu kriticheskoy informatsionnoy infrastruktury odnoy iz kategoriy znachimosti libo ob otsutstvii neobhodimosti prisvoeniya emu odnoy iz takih kategoriy* [On the approval of the form for sending information on the results of assigning a critical information infrastructure to the object of one of the importance categories or on the absence of the need to assign one of such categories to it]: the order of the Federal Service for Technical and Export Control dated December 22, 2017, no. 236 (in Russ.). Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (accessed: July 20, 2019).

Mikhail L. Soloviev
Acting Rector
Siberian State University of Telecommunications
and Information Sciences (SibSUTIS)
86, Kirov st., Novosibirsk, Russia, 630102
ORCID 0000-0002-4242-5571
Phone: +7 (383-2) 69-83-15
Email: miksol57@list.ru

Tatiana E. Mineeva
Graduate, Department of Information Systems Security,
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID 0000-0003-1702-8731
Phone: +7 (382-2) 70-15-29
Email: tatianamineeva7@gmail.com

Anton A. Konev
Candidate of Engineering Science, Assistant Professor,
Department of Integrated Information Security
of Electronic Computing Systems (KIBEVS), TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID 0000-0002-3222-9956
Phone: +7 (382-2) 70-15-29
Email: kaa1@keva.tusur.ru

Dmitriy N. Buintsev
Candidate of Engineering Science, Assistant Professor,
Department of Integrated Information Security
of Electronic Computing Systems (KIBEVS), TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 90-01-01
Email: buintsev-dn@tusur.ru