ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 004.056.53
DOI: 10.17586/0021-3454-2015-58-7-507-514

ЗАДАЧИ И МЕТОДЫ РЕЗЕРВИРОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. А. Щеглов, А. Ю. Щеглов

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: info@npp-itb.spb.ru

Исследованы задачи и возможности применения методов резервирования в области информационной безопасности. Введено понятие резервирования элементов информационной системы по угрозам атак. Выявлены фундаментальные противоречия методов резервирования, ограничивающие возможность их эффективного практического использования при решении задачи защиты информации в комплексе — защиты от нарушения конфиденциальности, доступности и целостности информации. Предложен метод резервирования элементов информационных систем с разделением процедуры обработки информации между элементами системы.

Ключевые слова: *резервирование, надежность, информационная безопасность, доступность информации, конфиденциальность информации, отказоустойчивость, угроза атаки.*

Введение. В работе [1] были введены базовые модели информационной безопасности, определяемые в терминах теории надежности, исследованы вопросы резервирования по угрозам уязвимости и по угрозам атак, вопросы проектирования систем защиты и их резервирования.

Резервирование является одним из эффективных способов повышения надежности функционирования информационной системы, при этом резервируются наиболее критичные к отказу элементы системы — как правило, серверы, на которых обрабатываются и хранятся данные [2—4].

Однако в современных условиях информационные системы, требующие резервирования элементов, т.е. критичные к нарушению характеристик надежности функционирования, подвержены угрозам атак реализации несанкционированного доступа, т.е. критичны и к нарушению характеристик информационной безопасности. Рассмотрим возможности применения известных методов резервирования элементов информационной системы применительно к решению задачи повышения уровня ее информационной безопасности. С учетом же того, что для современных информационных систем данные характеристики (надежности и информационной безопасности) одинаково важны, исследуем возможность комплексного решения задачи резервирования с использованием одних и тех же резервирующих средств в целях повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем (для повышения как уровня надежности, так и уровня информационной безопасности в комплексе).

При этом напомним [1] основные отличия в постановке данных задач резервирования. При резервировании, реализуемом в целях повышения надежности функционирования информационной системы, подразумевается, что исследуемыми событиями выступают отказы,

влияющие лишь на одну характеристику безопасности — надежность функционирования системы, при этом отказы зарезервированных элементов в общем случае (различные техногенные события не рассматриваются) можно интерпретировать как независимые события. В области информационной безопасности это не так.

1. Исследуемым событием безопасности является угроза атаки [1], при этом атаки, в отличие от отказа, не могут рассматриваться как независимые события, поскольку атака представляет собой не некое случайное, а осознанное деструктивное воздействие на информационную систему, реализуемое злоумышленником с целью несанкционированного доступа к обрабатываемой в системе информации. Естественно, что если злоумышленник совершил успешную атаку на элемент информационной системы, то в первую очередь он попытается совершить аналогичную апробированную им атаку на резервирующий элемент. Таким образом, деструктивные воздействия на зарезервированные элементы следует рассматривать как зависимые события.

2. Информационная безопасность имеет несколько ключевых характеристик, сопоставимо важных при решении задач повышения уровня информационной безопасности систем. К этим характеристикам относятся: защита от нарушения конфиденциальности информации (защита от ее хищения), защита от нарушения целостности информации (защита от ее несанкционированной модификации), защита от нарушения доступности информации [5]. В общем случае при реализации защиты информационной системы данные задачи защиты должны решаться в комплексе.

Задача резервирования элементов системы, решаемая в целях повышения надежности функционирования информационной системы. Данная задача решается за счет резервирования наиболее критичных к отказам элементов (как правило, серверов). Резервирующие элементы при этом в простейшем случае включаются по схеме параллельного резерва, в результате чего повышается вероятность того, что информационная система готова к эксплуатации ($P_{\text{г.э}}$). Вероятность $P_{\text{г.э}}$ определяется в предположении, что в системе используется V элементов с номерами v=1, …, V (V–1 из которых являются резервирующими элементами) при вероятности ($P_{\text{г.э}v}$) готовности v-го элемента к эксплуатации (отказы коммутирующих элементов для простоты не рассматриваются):

$$P_{\text{г.э}} = 1 - \prod_{v=1}^{V} (1 - P_{\text{г.э}v}).$$

Подобный эффект достигается благодаря тому, что при отказе одного из зарезервированных элементов информационная система продолжает функционировать. Для решения задачи оптимального резервирования ресурсов исследуются способы включения и использования в системе дополнительных элементов [3, 4].

В качестве резервирующих элементов могут применяться как полностью одинаковые, так и различные технические средства. Это обусловливается тем, что в общем случае отказы резервируемого и резервирующих элементов можно рассматривать как независимые события. Важным здесь является исключительно влияние характеристики $P_{\text{г.э}v}$ резервирующего элемента на характеристику $P_{\text{г.э}}$ информационной системы в целом.

Задачи резервирования элементов системы, решаемые в целях повышения уровня информационной безопасности системы. Как было отмечено ранее, информационная безопасность имеет несколько ключевых характеристик, здесь достаточно рассмотреть две из них — защиту от нарушения доступности информации и защиту от нарушения конфиденциальности информации.

Поскольку задачу повышения надежности функционирования информационной системы отчасти можно рассматривать в контексте обеспечения доступности информации (правда, отказ этой характеристики информационной безопасности в данном случае обусловливается не отказом оборудования, а реализацией успешной атаки, направленной на уничтожение

обрабатываемой в системе информации либо иных ресурсов, приводящих к невозможности получения доступа к информации), исследование вопросов резервирования элементов информационной системы начнем с ***задачи защиты от нарушения доступности обрабатываемой в системе информации***.

Повышение уровня защиты от нарушения доступности информации посредством резервирования возможно и достигается при использовании взаимонезависимых в отношении угроз атак элементов, т.е. при применении различных технических средств. Под различными будем понимать технические средства, для которых угрозы атак различны.

Обоснуем данное утверждение. Пусть каждый из V элементов, с номерами v=1, …, V, может быть представлен соответствующей характеристикой — вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, образующих угрозу безопасности элемента системы ($P_{0\text{у.э}v}$) [1].

В случае если все угрозы атак для всех V элементов различны, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, может быть определена следующим образом:

$$P_{0\text{у.э}V} = 1 - \prod_{v=1}^{V} (1 - P_{0\text{у.э}v}).$$

В случае если для повышения уровня защиты от нарушения доступности информации в качестве зарезервированных элементов применяются одинаковые технические средства, то резервирование элементов не реализуется. Под одинаковыми будем понимать технические средства, для которых угрозы атак одинаковы.

Докажем это положение. В случае если все угрозы атак для всех V элементов системы одинаковы, то вероятность $P_{0\text{у.э}V}$ с учетом того, что $P_{0\text{у.э}v=1} = P_{0\text{у.э}v=2} = \ldots = P_{0\text{у.э}v=V}$, может быть определена как

$$P_{0\text{у.э}V} = P_{0\text{у.э}v}.$$

Следствие. Резервирование элементов информационной системы применительно к задаче повышения уровня информационной безопасности можно представить соответствующей схемой резервирования в отношении угроз атак; при этом можно говорить о том, что задача резервирования элементов информационной системы сводится к задаче резервирования по угрозам атак [1].

Рассмотрим модель резервирования по угрозам атак. Если угрозы атак для всех элементов системы уникальны и характеризуются вероятностью $P_{0\text{у}r}$, r=1, ..., R (для соответствующих R зарезервированных элементов), того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможной атаки, то для реализации успешной атаки на систему в целом должна быть осуществлена успешная атака на каждый из зарезервированных элементов. В результате модель резервирования может быть представлена в виде орграфа (рис. 1, *а*), взвешенными вершинами которого являются вершины угроз атак на зарезервированные элементы, и соответствующей ему схемы параллельного резервирования (рис. 1, *б*).

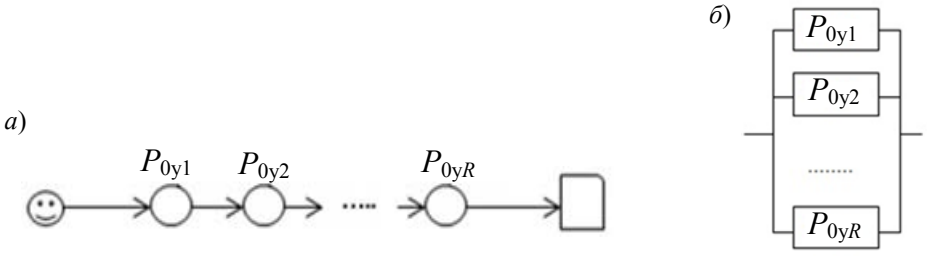

Рис. 1

Обозначим характеристику некой произвольной угрозы атаки как $P_{0\text{у}}$ (пусть рассматривается угроза подобной атаки на элемент системы v=1), для остальных элементов системы

v=2, ..., V соответствующую характеристику обозначим, как и прежде, — $P_{0\text{у.э}v}$; тогда соответствующая характеристика зарезервированной информационной системы может быть представлена следующим образом:

$$P_{0\text{у.э}V} = 1 - (1 - P_{0\text{у}}) \prod_{v=2}^{V} (1 - P_{0\text{у.э}v}).$$

Если одна и та же угроза атаки с характеристикой $P_{0\text{у}}$ одинакова, например, для элементов v=1, v=2, v=3 из V зарезервированных элементов, то получаем

$$P_{0\text{у.э}V} = 1 - (1 - P_{0\text{у}}) \prod_{v=4}^{V} (1 - P_{0\text{у.э}v}).$$

В предельном случае — если угроза атаки одинакова для всех зарезервированных элементов V, то

$$P_{0\text{у.э}V} = P_{0\text{у}},$$

т.е. применительно к подобной угрозе атаки задача резервирования не решается.

Следствия.

1. Задача резервирования элементов системы, применительно к решению задач повышения уровня ее информационной безопасности для защиты от нарушения доступности информации, сводится к задаче резервирования угроз атак на элемент информационной системы.

2. При полном совпадении резервируемого и резервирующего элементов информационной системы задача резервирования элементов не решается, поскольку в данном случае не реализуется резервирование по угрозам атак.

Приведенные соображения позволяют ввести понятие и количественную оценку актуальности угрозы атаки [1], но уже на зарезервированную информационную систему. Под количественной оценкой актуальности угрозы атаки на зарезервированную информационную систему будем понимать вероятность готовности системы к безопасной эксплуатации в отношении этой атаки — $P_{0\text{у.э}v}$. Естественно, что к наиболее актуальным в общем случае относятся угрозы атак, актуальные и для резервируемого, и для резервирующих элементов информационной системы. Именно в отношении подобных угроз атак при резервировании элементов в первую очередь потребуется применить средства защиты, направленные на повышение значения характеристики $P_{0\text{у.э}v}$ [1].

Задача защиты от нарушения доступности информации, которое может быть вызвано как отказом элемента системы, так и реализацией атаки на этот элемент злоумышленником, может решаться в комплексе. При этом, с точки зрения повышения надежности информационной системы, проектирование зарезервированной системы должно проводиться с учетом требований к максимальному различию резервируемого и резервирующих элементов с целью выполнения требования к уникальности угроз атак на эти элементы системы. Как следствие, задача повышения уровня интегрированной информационно-эксплуатационной безопасности информационной системы предполагает вполне определенную постановку задачи повышения ее надежности (отказоустойчивости) посредством резервирования элементов системы.

Обратимся теперь к другой характеристике информационной безопасности — ***защите от нарушения конфиденциальности информации, обрабатываемой в системе***.

Конфиденциальность информации может быть нарушена в результате реализации злоумышленником атаки на информационную систему, но уже с целью хищения обрабатываемой в ней информации.

Применительно к данной задаче защиты резервирование элементов информационной системы опять же можно представить в виде орграфа и соответствующей ему схемы резервирования, в данном случае последовательного резервирования, в отношении угроз атак [1].

Рассмотрим модель резервирования по угрозам атак при решении данной задачи. Если угрозы атак для всех зарезервированных элементов системы уникальны и характеризуются

известной (введенной ранее) вероятностью P_{0yr}, r=1, ..., R, то в этом случае при осуществлении успешной атаки на любой из зарезервированных элементов обрабатываемая информация будет похищена. В результате формируется орграф и соответствующая ему схема последовательного резервирования (рис. 2, *а*, *б*).

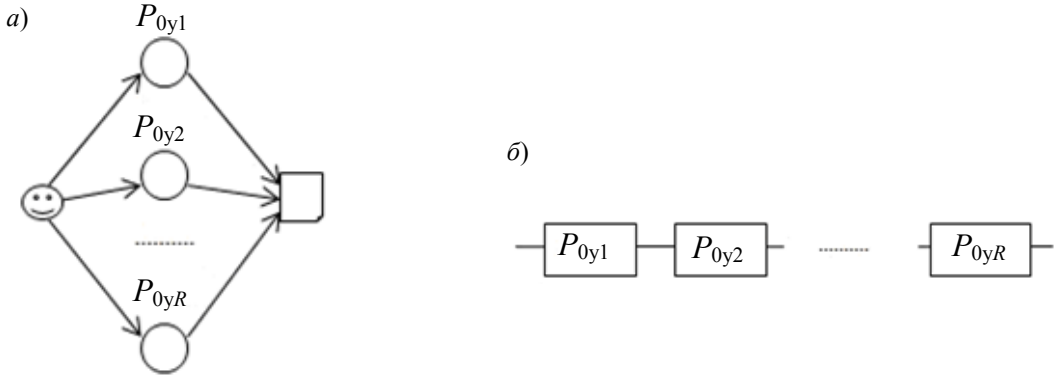

Рис. 2

Повышение уровня защиты от нарушения конфиденциальности информации посредством резервирования принципиально невозможно, поскольку в данном случае невозможно резервирование по угрозам атак.

Обоснуем данное утверждение. Пусть каждый из V зарезервированных элементов, с номерами v=1, …, V, может быть представлен соответствующим орграфом угроз атак и соответствующей характеристикой — вероятностью $P_{0y.эv}$.

В случае если все угрозы атак для V элементов системы одинаковы (не зарезервированы), при этом для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то вероятность $P_{0y.эV}$ с учетом того, что $P_{0y.эv=1} = P_{0y.эv=2} = \ldots = P_{0y.эv=V}$, определяется (как и в предыдущем случае) следующим образом:

$$P_{0y.эV} = P_{0y.эv}. \qquad (1)$$

В случае если все угрозы атак для V элементов системы различны (зарезервированы), при этом для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то

$$P_{0y.эV} = \prod_{v=1}^{V} P_{0y.эv}. \qquad (2)$$

Решение задачи повышения уровня безопасности информационной системы для защиты от нарушения доступности информации посредством резервирования приводит к снижению уровня безопасности системы при защите от нарушения конфиденциальности информации.

Как отмечалось ранее, повышение уровня защиты от нарушения доступности информации посредством резервирования возможно и достигается только при максимальном различии резервирующих и резервируемого элементов по угрозам атак, но именно при этих условиях снижается уровень безопасности информационной системы для защиты от нарушения конфиденциальности информации.

Резюмируя вышеизложенное, можно сделать следующие выводы.

1. Применение методов резервирования для повышения уровня безопасности информационной системы связано с фундаментальным противоречием, состоящим в том, что задачи защиты от нарушения доступности информации и защиты от нарушения конфиденциальности информации не то что не могут решаться в комплексе, но и более того, улучшение одной из этих характеристик информационной безопасности в результате реализации резервирования по угрозам атак на элементы системы приводит к ухудшению другой характеристики, что недопустимо вследствие одинаковой важности данных характеристик для современных информационных

систем. В этом смысле известные методы резервирования не могут быть эффективно использованы в области информационной безопасности. Выявленные противоречия методов резервирования могут быть отнесены к фундаментальным, так как они не связаны с какими-либо характеристиками защищаемых информационных систем, используемым в них оборудованием, программными средствами и т.д. Данные противоречия обусловливаются собственно постановкой задачи резервирования элементов информационных систем в области информационной безопасности как задачи резервирования по угрозам атак на элементы систем.

2. Эффективное решение задачи повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем посредством резервирования возможно только при реализации защиты от нарушения доступности информации. В данном случае задача повышения безопасности решается резервированием угроз атак, однако при этом ухудшается важнейшая характеристика информационной безопасности системы — конфиденциальность обрабатываемой информации.

3. Поскольку в современных информационных системах задачи повышения эксплуатационной и информационной безопасности, и в частности задачи повышения уровня конфиденциальности и доступности информации, должны решаться в комплексе, а известные методы резервирования для этого не эффективны, необходима разработка новых, принципиально иных подходов к резервированию элементов информационных систем, позволяющих учесть выявленные фундаментальные противоречия существующих методов.

Метод резервирования с распределением информации между элементами системы. Как показало проведенное выше исследование, резервирование для решения задачи повышения уровня конфиденциальности обрабатываемой в системе информации не может использоваться. Поэтому рассмотрим данную задачу с позиций оценки риска потенциальных потерь [6]. Риск потенциальных потерь G_C применительно к угрозе безопасности информационной системы (характеристика $P_{0\text{у.э}V}$) в простейшем случае (без учета эксплуатационных характеристик системы [6, 7]) можно оценить как

$$G_C = C_{\text{инф}}(1 - P_{0\text{у.э}V}).$$

Характеристика потерь $C_{\text{инф}}$ зависит от объема похищенной информации, поэтому введем характеристику удельной стоимости $C_{\text{уд}}$ единицы информации. Исходя из того, что в системе обрабатывается N единиц информации, величину потерь, обусловливаемых хищением обрабатываемой информации, можно определить следующим образом:

$$C_{\text{инф}} = C_{\text{уд}}N.$$

С учетом подобной интерпретации задача повышения посредством резервирования элементов системы уровня ее эксплуатационной и информационной безопасности, применительно к защите от нарушения конфиденциальности информации, может рассматриваться как задача снижения потерь от реализации успешной атаки на элемент системы при распределении информации между зарезервированными элементами. Задача резервирования в данном случае предполагает разделение процедур хранения и обработки информации между V элементами; при равном распределении между V элементами объемов обрабатываемой информации каждый из них будет концентрировать информацию стоимостью $C_{\text{инф}v}$:

$$C_{\text{инф}v} = C_{\text{уд}}N / V.$$

Следовательно, реализация успешной атаки на один из зарезервированных элементов системы соответствует $C_{\text{инф}v}$, что снизит потери от успешной атаки в V раз.

Подобный метод резервирования назовем „методом резервирования с распределением обрабатываемой информации между элементами системы“.

Повышение уровня защиты от нарушения конфиденциальности информации с помощью данного метода резервирования возможно и достигается только в случае резервирования по угрозам атак.

Докажем это утверждение. В случае если все угрозы атак для V элементов системы одинаковы, т.е. на все V зарезервированных элементов может быть осуществлена одна и та же атака (резервирование по угрозам атак не реализовано), то риск потерь от реализации угрозы атаки на элемент системы (характеристика $P_{0\text{у.эv}}$) рассчитывается следующим образом:

$$G_C = C_{\text{инф}}(1 - P_{0\text{у.эv}}).$$

В случае же если все угрозы атак для V элементов различны (зарезервированы), т.е. одна и та же атака может быть осуществлена только на один из V зарезервированных элементов, тогда

$$G_C = C_{\text{инф}}(1 - P_{0\text{у.эv}})/V.$$

Представленные выше формулы для рассмотренных альтернативных случаев доказывают, что повышение уровня защиты от нарушения конфиденциальности информации путем резервирования возможно и достигается только в случае, когда применяются взаимонезависимые в отношении угроз атак элементы, при этом одинаковые элементы не могут использоваться, посредством их резервирования, в целях повышения уровня защиты от нарушения конфиденциальности информации.

Применение предлагаемого метода (в случае реализации резервирования по угрозам атак), позволяющего снизить риск потенциальных потерь от осуществления успешной атаки на элемент системы (в V раз*)*, приводит к увеличению риска частичных потерь информации, обрабатываемой в системе, т.е. потерь информации в объеме, обрабатываемом одним из зарезервированных элементов системы.

Обоснуем данное противоречие. Как было показано ранее, если все угрозы атак для V зарезервированных элементов системы различны (зарезервированы), то справедливо выражение (2); в случае же если все угрозы атак для V резервируемых элементов одинаковы (не зарезервированы), справедливо равенство (1). Однако в этом случае поскольку на все V зарезервированных элементов системы может быть осуществлена одна и та же успешная атака, уже следует говорить о риске хищения всей обрабатываемой в системе информации и о соответствующем для этого случая риске потерь.

Данное противоречие — снижение риска хищения информации, обрабатываемой в системе в полном объеме, при одновременном увеличении риска хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, — можно признать принципиальным противоречием метода резервирования с распределением обрабатываемой информации между элементами системы. Это крайне важное противоречие обязательно должно учитываться при разработке требований к характеристикам и параметрам средств защиты информации [1], реализуемых (при необходимости) для резервируемых элементов информационной системы.

Предложенный метод резервирования позволяет повысить уровень информационной безопасности при реализации как защиты от нарушения доступности информации, так и защиты от нарушения ее конфиденциальности.

Заключение. Представленное исследование иллюстрирует фундаментальные противоречия и принципиальную невозможность решения задачи повышения уровня информационной безопасности информационной системы с использованием известных из теории надежности [2] методов резервирования при решении задачи защиты информации в комплексе — защиты от нарушения конфиденциальности, доступности и целостности информации. В качестве альтернативного решения предложен метод резервирования элементов информационных систем с распределением обрабатываемой информации между элементами системы.

СПИСОК ЛИТЕРАТУРЫ

1. *Щеглов К. А., Щеглов А. Ю.* Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. № 3, вып. 106. С. 52—65.

2. *Половко А. М., Гуров С. В.* Основы теории надежности. СПб: БХВ-Петербург, 2006.

3. *Богатырев В. А.* Надежность и эффективность резервированных компьютерных сетей // Информационные технологии. 2006. № 9. С. 25—30.

4. *Богатырев В. А., Богатырев С. В., Богатырев А. В.* Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения // Информационные технологии. 2013. № 2. С. 27—32.

5. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Введ. 18.12.2008. М.: Стандартинформ, 2009.

6. *Щеглов К. А., Щеглов А. Ю.* Эксплуатационные характеристики риска нарушений безопасности информационной системы // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 1(89). С. 129—139.

7. *Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А.* Основы информационной безопасности. М.: Горячая линия — Телеком, 2006.

Сведения об авторах

Константин Андреевич Щеглов — аспирант; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 06.02.15 г.

Ссылка для цитирования: *Щеглов К. А., Щеглов А. Ю.* Задачи и методы резервирования в области информационной безопасности // Изв. вузов. Приборостроение. 2015. Т. 58, № 7. С. 507—514.

PROBLEMS AND METHODS OF RESERVATION IN INFORMATION SECURITY

K. A. Shcheglov, A. Yu. Shcheglov

ITMO University, 197101, Saint Petersburg, Russia
E-mail: info@npp-itb.spb.ru

The problems and potentialities of reservation methods application in the field of informational security are considered. A concept of reservation of information system elements relative to threats of attack is introduced. Internal contradictions of reservation methods are revealed. The contradictions are shown to limit practical applicability of the methods to the complete problem of information protection, including confidentiality support, save access to the information, and data integrity. A method is proposed for reservation of information system elements with division of information processing procedure between the system elements.

Keywords: backup, reliability, information security, operational security, integrated security, information accessibility, confidential information, element resiliency, threat of attack.

Data on authors

Konstantin A. Shcheglov — Post-Graduate Student; ITMO University; Department of Computer Science, E-mail: info@npp-itb.spb.ru

Andrey Yu. Shcheglov — Dr. Sci., Professor; ITMO University; Department of Computer Science, E-mail: info@npp-itb.spb.ru

Reference for citation: *Shcheglov K. A., Shcheglov A. Yu.* Problems and methods of reservation in information security // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2015. Vol. 58, N 7. P. 507—514 (in Russian).

DOI: 10.17586/0021-3454-2015-58-7-507-514