УДК 004.056.53

К. А. Щеглов, аспирант, **А. Ю. Щеглов,** д-р техн. наук, проф., e-mail: indo@npp-itb.spb.ru,
Национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербург, Россия

Возможности методов резервирования для повышения уровня интегрированной информационно-эксплуатационной безопасности современных информационных систем

Исследованы вопросы резервирования элементов информационной системы в области информационной безопасности. Проиллюстрированы принципиальные особенности постановки задачи резервирования элементов информационной системы, решаемой в целях повышения надежности функционирования и уровня информационной безопасности. Выявлены и обоснованы фундаментальные противоречия использования методов резервирования в области информационной безопасности, ограничивающие возможность их эффективного практического использования при решении задач защиты информации — повышение уровня конфиденциальности, целостности и доступности обрабатываемой информации в комплексе, а также противоречия, не позволяющие эффективно решать известными методами резервирования в комплексе задачи повышения надежности функционирования и уровня информационной безопасности информационной системы. Предложен метод резервирования с разделением обрабатываемой информации между элементами информационной системы, позволяющий решать задачи повышения уровня интегрированной информационно-эксплуатационной безопасности, дана оценка его эффективности.

Ключевые слова: *информационная система, резервирование, надежность, отказоустойчивость, информационная безопасность, доступность информации, конфиденциальность информации, целостность информации, отказоустойчивость, информационно-эксплуатационная безопасность*

Введение

В общем случае резервирование широко применяется на практике в целях повышения надежности функционирования информационной системы, при этом резервируются наиболее критичные к отказу элементы информационной системы, как правило, серверы, на которых концентрируется обработка и хранение обрабатываемых данных [1—3].

Резервирующие элементы при этом в простейшем случае включаются по схеме параллельного резерва, в результате чего повышается вероятность того, что информационная система готова к эксплуатации ($P_{\text{гэ}}$). В предположении того, что в системе используется V элементов с номерами $v = 1, ..., V$ ($V - 1$ из которых являются резервирующими элементами) при вероятности готовности v-го элемента к эксплуатации ($P_{\text{гэ}v}$) вероятность $P_{\text{гэ}}$ определяется следующим образом (отказы коммутирующих элементов для простоты не рассматриваем):

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

Однако трудно себе представить, чтобы в современных условиях информационные системы, требующие резервирования элементов, т. е. критичные к нарушению характеристики надежности функционирования, не были подвержены угрозам атак несанкционированного доступа. Так же, как и вопросы надежности функционирования, — это вопросы безопасности, но уже не эксплуатационной, а иной — информационной. Как следствие, при проектировании современных информационных систем с резервированием их элементов задачи повышения уровня безопасности информационных систем следует рассматривать в комплексе (с позиции эксплуатационных характеристик и характеристик информационной безопасности), ставя и решая задачу повышения уровня интегрированной информационно-эксплуатационной безопасности.

Рассмотрим, в чем состоит особенность постановки задачи резервирования элементов информационной системы в целях повышения уровня информационной безопасности, а также, какие методы резервирования могут применяться для комплексного решения задачи — задачи повышения уровня интегрированной информационно-эксплуатационной безопасности.

Особенности постановки задачи резервирования в целях повышения уровня информационной безопасности информационной системы

Говоря о резервировании, реализуемом в целях повышения надежности функционирования некоторой системы, мы подразумеваем, что исследуемыми событиями выступают отказы, влияющие лишь на одну характеристику — характеристику надежности функционирования системы. При этом отказы зарезервированных элементов в общем случае (не рассматриваем различные техногенные события) можно интерпретировать как независимые события. В информационной безопасности все не так.

1. Исследуемым элементом безопасности в информационной системе является угроза атак, при этом атаки, в отличие от отказов, никак не могут рассматриваться как независимые события, поскольку атака представляет собой не некое случайное, а осознанное деструктивное воздействие злоумышленника на информационную систему в целях реализации несанкционированного доступа. Естественно, что если злоумышленник совершил успешную атаку на элемент информационной системы, он также попытается совершить аналогичную атаку на резервирующий элемент.

2. Информационная безопасность имеет несколько ключевых характеристик. К характеристикам информационной безопасности 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 [4].

В общем случае, при реализации эффективной защиты информационной системы, данные задачи защиты должны решаться в комплексе.

С учетом сказанного рассмотрим задачи и возможности резервирования элементов информационной системы с позиций повышения уровня именно ее информационной безопасности. При этом будем исследовать альтернативные варианты резервирования:

- резервирующий элемент по атакам полностью независим от резервируемого элемента (угрозы атак для резервируемого и резервирующего элемента полностью различны);
- резервирующий элемент по атакам полностью зависим от резервируемого элемента (угрозы атак для резервируемого и резервирующего элемента полностью совпадают).

Замечание. На практике, как правило, крайне затруднительно обеспечить полную независимость резервирующего элемента по атакам от резервируемого, поскольку в общем случае это предполагает использование различного оборудования и полностью различного программного обеспечения для резервируемого и резервирующих элементов, что подчас бывает не выполнимо.

Резервирование в целях защиты от нарушения доступности информации

Утверждение. Повышение уровня защиты от нарушения доступности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам).

Доказательство. Пусть каждый из V зарезервированных элементов с номерами $v = 1, ..., V$ может быть представлен соответствующей характеристикой — вероятностью $P_{0\text{уэ}v}$ того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, образующих угрозу безопасности элемента информационной системы [5, 6].

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

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

В случае же если все угрозы атак для всех V зарезервированных элементов системы зависимы (угрозы атак соответствующим образом совпадают для всех элементов), то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, с учетом того, что $P_{0\text{уэ}v=1} = P_{0\text{уэ}v=2} = ... = P_{0\text{уэ}v=V}$, может быть определена следующим образом:

$$P_{0\text{уэ}V} = P_{0\text{уэ}v}.$$

Представленные выше формулы для альтернативных рассмотренных случаев доказывают, что повышение уровня защиты от нарушения доступности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам). При этом резервирование элемента полностью идентичными элементами не может рассматриваться в качестве резервирования элемента информационной системы в целях повышения уровня защиты от нарушения доступности информации.

Следствие 1.

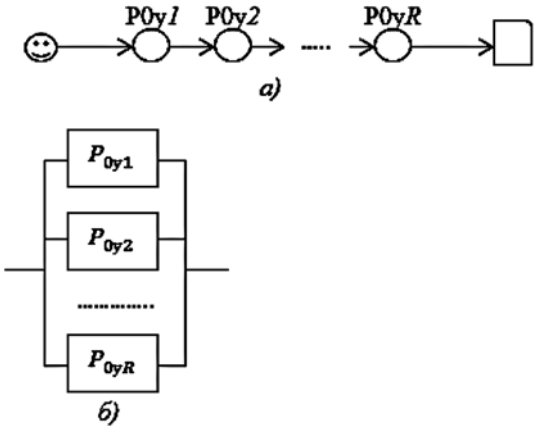
С учетом сказанного резервирование элементов информационной системы в части повышения уровня информационной безопасности можно интерпретировать соответствующей схемой резервирования в отношении угроз атак. При этом если угрозы атак всех зарезервированных элементов системы уникальны (независимы) и характеризуются вероятностью P_{0yr}, $r = 1, ..., R$, (для соответствующих R зарезервированных элементов), то для успешной атаки на информационную систему в целом должна быть осуществлена успешная атака на каждый из резервирующих элементов (реализованы угрозы информационной безопасности всех резервирующих элементов). В результате сказанного получаем орграф (см. рисунок), взвешенными вершинами которого выступают вершины угроз атак зарезервированных элементов, и соответствующую ему схему параллельного резервирования.

Обозначим характеристику некой произвольной угрозы атаки как P_{0y} (пусть рассматриваем угрозу подобной атаки на элемент системы $v = 1$), для остальных элементов системы $v = 2, ..., V$ обозначаем соответствующую характеристику, как и прежде, $P_{0yэv}$. В данных предположениях соответствующая характеристика зарезервированной информационной системы $P_{0yэv}$ может быть представлена следующим образом:

$$P_{0yэV} = 1 - (1 - P_{0y}) \prod_{v=2}^{V} (1 - P_{0yэv}).$$

Если же одна и та же угроза атаки с характеристикой P_{0y} совпадает, например, для элементов $v = 1$, $v = 2$, $v = 3$ из V зарезервированных элементов, то для $P_{0yэV}$ получаем:

$$P_{0yэV} = 1 - (1 - P_{0y}) \prod_{v=4}^{V} (1 - P_{0yэv}).$$



Орграф угрозы атак на информационную систему и схема резервирования:
а — орграф угроз атак; *б* — схема параллельного резервирования

В пределе, когда угроза атаки совпадает для всех зарезервированных элементов V, имеем:

$$P_{0yэV} = P_{0y},$$

т. е. в данном случае — применительно к подобной угрозе атаки — задача резервирования не решается.

Следствие 2.

Задача резервирования элементов информационной системы применительно к решению задач повышения уровня эксплуатационной информационной безопасности информационных систем в части защиты от нарушения доступности информации сводится к задаче резервирования угроз атак на элемент информационной системы посредством резервирования данного элемента элементом (элементами), характеризуемым иными (уникальными) угрозами атак.

Сказанное позволяет ввести понятие и количественную оценку актуальности угрозы атаки [5, 6], но уже на зарезервированную информационную систему (на зарезервированный элемент информационной системы).

Под количественной оценкой актуальности угрозы атаки на зарезервированную информационную систему (на зарезервированный элемент информационной системы) будем понимать значение вероятности $P_{0yэv}$ готовности к безопасной эксплуатации зарезервированной информационной системы в отношении этой атаки. Естественно, что к наиболее актуальным угрозам атак в результате резервирования элементов информационной системы в общем случае будут отнесены нерезервируемые угрозы атак — угрозы атак, актуальные и для резервируемого, и для резервирующих элементов информационной системы. Именно в отношении подобных угроз атак при резервировании элементов информационной системы, в первую очередь, потребуется применение средств защиты, направленных на повышение значения характеристики $P_{0yэv}$ [6].

Поскольку, как отмечали выше, трудно себе представить современную информационную систему, в которой решаются задачи резервирования элементов в целях повышения ее надежности без необходимости повышения уровня эксплуатационной информационной безопасности подобной системы, то в части защиты от нарушения доступности информации, которое может быть вызвано как отказом элемента системы, так и реализацией атаки на этот элемент злоумышленником, можно формулировать и решать задачу защиты от нарушения доступности информации в комплексе и при этом говорить об интегрированной информационно-эксплуатационной безопасности информационных систем. При этом с точки зрения повышения надежности информационной системы проектирование зарезервированной системы должно проводиться с учетом

требований к максимальному различию (а это и вопросы отказоустойчивости, и вопросы производительности) резервируемого и резервирующих элементов. Другими словами, решение задач повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем предполагает вполне определенную формулировку задачи повышения надежности информационных систем посредством резервирования ее элементов.

Резервирование в целях защиты от нарушения конфиденциальности информации

Применительно к данной задаче защиты резервирование элементов информационной системы опять же можно интерпретировать соответствующим орграфом и соответствующей схемой, но уже последовательного резервирования [5, 6].

Утверждение. Повышение уровня защиты от нарушения конфиденциальности информации резервированием невозможно.

Доказательство. Особенность резервирования элементов информационной системы в данном случае состоит в том, что информация может быть похищена злоумышленником как с резервируемого, так и с резервирующих элементов.

Пусть каждый из V зарезервированных элементов с номерами $v = 1, ..., V$ может быть представлен соответствующим орграфом угроз безопасности элемента информационной системы и соответствующей характеристикой — вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, образующих угрозу безопасности элемента информационной системы ($P_{0\text{уэ}v}$) [5, 6].

В случае если все угрозы атак в V резервируемых элементах системы зависимы (полностью совпадают) и для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак ($P_{0\text{уэ}V}$), с учетом того, что $P_{0\text{уэ}v=1} = P_{0\text{уэ}v=2} = ... = P_{0\text{уэ}v=v}$, в данных предположениях может быть определена следующим образом:

$$P_{0\text{уэ}V} = P_{0\text{уэ}v}.$$

В случае же если все угрозы атак в V зарезервированных элементах системы независимы (соответствующим образом различаются во всех элементах) и для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак ($P_{0\text{уэ}V}$), определяется формулой

$$P_{0\text{уэ}V} = \prod_{v=1}^{V} P_{0\text{уэ}v}.$$

Представленные выше формулы для альтернативных рассмотренных случаев доказывают, что повышение уровня защиты от нарушения конфиденциальности информации резервированием невозможно.

Утверждение. Решение задачи повышения уровня защиты от нарушения доступности информации резервированием приводит к снижению уровня защиты от нарушения конфиденциальности информации.

Доказательство. Как отмечали выше, повышения уровня защиты от нарушения доступности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам), но именно при этих условиях снижается уровень защиты от нарушения конфиденциальности информации.

Следствие 3.

Резервирование для решения задачи повышения уровня информационной безопасности в части защиты от нарушения конфиденциальности информации не имеет смысла.

Следствие 4.

Задача повышения резервированием элементов информационной системы уровня информационной безопасности в части защиты от нарушения доступности информации вступает в противоречие с задачей повышения уровня информационной безопасности в части защиты от нарушения конфиденциальности информации, поскольку повышением уровня информационной безопасности в части защиты от нарушения доступности информации снижается уровень информационной безопасности в части защиты от нарушения конфиденциальности информации.

Метод резервирования, направленный на повышение уровня интегрированной информационно-эксплуатационной безопасности

С позиций необходимости решения задачи повышения резервированием элементов информационной системы уровня информационной безопасности в части защиты от нарушения конфиденциальности информации обратимся к оценке эксплуатационного риска потенциальных потерь [5]. Риск потерь $R_{C_{\text{у. инф}}}$ применительно к угрозе безопасности информационной системы (характеристика угрозы

безопасности информационной системы $P_{0\text{уэ}V}$) в простейшем случае (без учета эксплуатационных характеристик информационной системы [5]) можно оценить следующим образом:

$$R_{C_{\text{у.инф}}} = C_{\text{инф}}(1 - P_{0\text{уэ}V}),$$

где $C_{\text{инф}}$ — потенциальные потери от хищения конфиденциальной информации.

Пусть характеристика $C_{\text{инф}}$ зависит от объема похищенной информации, т. е. введем характеристику удельной стоимости $C_{\text{у.инф}}$ единицы информации. Исходя из того, что в информационной системе обрабатывается N единиц информации, характеризуемых удельной стоимостью $C_{\text{у.инф}}$, величину потерь, обусловливаемых хищением обрабатываемой в информационной системе информации, можем представить следующим образом:

$$C_{\text{инф}} = C_{\text{у.инф}}N.$$

С учетом подобного представления задача повышения с помощью резервирования элементов информационной системы уровня эксплуатационной информационной безопасности в части защиты от нарушения конфиденциальности информации может рассматриваться как задача снижения потерь от реализации успешной атаки на элемент информационной системы. Задача резервирования в данном случае будет предполагать разделение хранения и обработки информации между V зарезервированными элементами информационной системы. При равном распределении между V элементами объемов обрабатываемой информации на каждом из них будет сконцентрирована информация стоимостью $C_{\text{инф}v}$:

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

Следовательно, реализация успешной атаки на один из зарезервированных элементов информационной системы снизит потери в V раз.

Назовем подобный метод резервирования "методом резервирования с разделением обрабатываемой информации".

Утверждение. Повышение уровня защиты от нарушения конфиденциальности информации методом резервирования с разделением обрабатываемой информации возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам).

Доказательство. В случае если все угрозы атак в V резервируемых элементах системы зависимы (соответствующим образом полностью совпадают, т. е. одна и та же атака может быть реализована на все V зарезервированных элемента), риск потерь от реализации угрозы на элемент системы (характеристика угрозы атаки на элемент системы $P_{0\text{уэ}v}$) рассчитывается следующим образом:

$$R_{C_{\text{у.инф}}} = C_{\text{инф}}(1 - P_{0\text{уэ}v}).$$

В случае же если все угрозы атак в V резервируемых элементах системы не зависимы (соответствующим образом различаются во всех элементах, одна и та же атака может быть реализована только на один из V зарезервированный элемент), имеем:

$$R_{C_{\text{у.инф}}} = C_{\text{инф}}(1 - P_{0\text{уэ}v})/V.$$

Представленные выше формулы для альтернативных рассмотренных случаев доказывают, что повышение уровня защиты от нарушения конфиденциальности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам), при этом резервирование элемента полностью идентичными элементами не может рассматриваться в качестве резервирования элемента информационной системы в целях повышения уровня защиты от нарушения конфиденциальности информации.

Замечание. Метод резервирования с разделением обрабатываемой информации имеет одно очень важное свойство. С одной стороны, эффективность резервирования в данном случае достигается тогда, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам). При этом снижается вероятность потерь, связанных с нарушением конфиденциальности всей обрабатываемой информации, стоимость которой $C_{\text{инф}}$, поскольку любая успешная атака на зарезервированную систему приводит лишь к частичным потерям, стоимость которых определяется как $C_{\text{инф}v}$. С другой же стороны, ранее это было показано (и доказано), при таких условиях (когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак) снижается уровень защиты от частичных потерь, стоимость которых определяется как $C_{\text{инф}v}$, поскольку повышается вероятность реализации успешной атаки на один из V зарезервированных элементов.

Это крайне важное противоречие метода резервирования с разделением обрабатываемой информации, которое в обязательном порядке должно учитываться при разработке требований к характеристикам и параметрам средств защиты [6], реализуемых (при необходимости) в резервируемых эле-

ментах информационной системы. Итак, задачи повышения резервированием элементов информационной системы уровня эксплуатационной информационной безопасности как в части защиты от нарушения доступности информации, так и в части защиты от нарушения конфиденциальности информации (при реализации метода резервирования с разделением обрабатываемой информации) решаются в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам).

Утверждение. Метод резервирования с разделением обрабатываемой информации позволяет повышать резервированием элементов информационной системы уровень информационной безопасности как в части защиты от нарушения доступности информации, так и в части защиты от нарушения конфиденциальности информации.

Доказательство. Данное утверждение в отношении применения метода резервирования с разделением обрабатываемой информации доказывается тем, что обе задачи защиты решаются в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам). То есть требования к решению данных задач защиты не противоречат друг другу.

Утверждение. Метод резервирования с разделением обрабатываемой информации может применяться для решения задач повышения уровня интегрированной информационно-эксплуатационной безопасности.

Доказательство. Данное утверждение в отношении применения метода резервирования с разделением обрабатываемой информации доказывается тем, что обе задачи (задача повышения надежности функционирования и задача повышения уровня информационной безопасности) решаются в том случае, когда применяются резервирующие элементы, не зависимые между собой и с резервируемым элементом по угрозам атак (по потенциально возможным атакам). То есть требования к решению данных задач резервирования не противоречат друг другу. Как следствие, они могут решаться в комплексе.

Отметим, что особенностью реализации метода резервирования с разделением обрабатываемой информации является то, что реализация успешной атаки на зарезервированный элемент информационной системы приводит лишь к частичным потерям конфиденциальности информации и соответственно лишь к частичным потерям доступности информации. Лишь к частичным потерям доступности информации приводит и отказ зарезервированного элемента информационной системы. То есть данный метод резервирования пусть частично (не в полном объеме), но позволяет решать задачи повышения уровня интегрированной информационно-эксплуатационной безопасности в комплексе.

Заключение

Отметим, что проведенные в работе исследования иллюстрируют, насколько различны даже собственно в своей постановке задачи резервирования, решаемые в целях повышения уровня надежности функционирования и уровня информационной безопасности информационных систем. Проиллюстрированы и ключевые противоречия применения известных методов резервирования, состоящие в возможности улучшения одних характеристик за счет ухудшения других характеристик информационной системы, что недопустимо для практического применения, поскольку для современных информационных систем нельзя подобные альтернативные задачи резервирования рассматривать не в комплексе. В качестве компромиссного решения может рассматриваться предложенный в работе метод резервирования с разделением обрабатываемой информации, который пусть частично (не в полном объеме), но позволяет решать задачи повышения уровня интегрированной информационно-эксплуатационной безопасности.

Список литературы

1. **Половко А. М., Гуров С. В.** Основы теории надежности. СПб.: БХВ-Петербург. 2006. 704 с.

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

3. **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.

4. **ГОСТ** Р 53114—2008. Защита информации. Обеспечение информационной безопасности в организации, 2009.

5. **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.

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

K. A. Shcheglov, Graduate Student, **A. Yu. Shcheglov,** Professor, e-mail: info@npp-itb.spb.ru,
St. Petersburg National research university of IT, Mechanics and Optics, Russia

The Reservation Methods Capabilities to Enhance Integral Information and Operational Security Level of Modern Informational Systems

We do research informational system elements reservation problem. We do illustrate the principal difference of setting the task for informational system elements reservation (to enhance functional reliability and informational security level). We identified and justified the fundamental contradictions of using reservation methods in informational security, which place limits on their effective practical usage while solving information security problems like enhancing confidential level, integrity and availability of information, including contradictions, which prevent effective solutions based on known reservation methods (in context of functional reliability and informational system security level enhancing problem). We do suggest the reservation method with dividing information between informational system elements, which allows to solve problem of enhancing integral information and operational security level and also define an assessment of its effectiveness.

Keywords: *informational system, reservation, reliability, resiliency, informational security, information accessibility, confidential information, information integrity, information operational security*

References

1. **Polovko A. M., Gurov S. V.** *Osnovy teorii nadezhnosti.* SPb.: BHV-Peterburg. 2006. 704 p.
2. **Bogatyrev V. A.** Nadezhnost' i jeffektivnost' rezervirovannyh komp'juternyh setej. *Informacionnye tehnologii.* 2006. N. 9. P. 25—30.
3. **Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V.** Nadezhnost' klasternyh vychislitel'nyh sistem s dublirovannymi svjazjami serverov i ustrojstv hranenija. *Informacionnye tehnologii.* 2013. N. 2. P. 27—32.
4. **GOST** R 53114—2008. *Zashhita informacii. Obespechenie informacionnoj bezopasnosti v organizacii*, 2009.
5. **Shcheglov K. A., Shcheglov A. Ju.** Jekspluatacionnye harakteristiki riska narushenij bezopasnosti informacionnoi sistemy. *Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki.* 2014. N. 1 (89). P. 129—139.
6. **Shcheglov K. A., Shcheglov A. Ju.** Matematicheskie modeli jekspluatacionnoj informacionnoj bezopasnosti. *Voprosy zashhity informacii.* 2014. Vyp. 106. N. 3. P. 52—65.

УДК 004.023

М. А. Перегудов, адъюнкт, e-mail: maxaperegudov@mail.ru,
А. А. Бойко, канд. техн. наук, доц., зам. нач. отдела, e-mail: algeminy@mail.ru,
Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина" (г. Воронеж)

Оценка защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA

Предложена математическая модель, позволяющая оценить защищенность сети пакетной радиосвязи от деструктивных воздействий, направленных на имитацию абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA.

Ключевые слова: *сеть пакетной радиосвязи, S-ALOHA, деструктивное воздействие, марковская модель, защищенность*

Введение

Современные сети пакетной радиосвязи (СПР) нередко подвергаются деструктивным воздействиям [1], целью которых является нарушение конфиденциальности, целостности и доступности информации. Одним из основных способов деструктивных воздействий на СПР является имитация злоумышленником ложных соединений от имени абонентских терминалов (АТ).

На начальном этапе информационного взаимодействия установление соединения между АТ и средством коммутации и управления (СКУ) в СПР реализуется в процедуре случайного множественного