БЕЗОПАСНОСТЬ ИНФОРМАЦИИ
CRYPTOSAFETY INFORMATION

УДК 004.056.53

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

Интерпретация и моделирование угрозы атаки на информационную систему. Часть 1. Моделирование угрозы уязвимости и интерпретация угрозы атаки

Введена классификация угроз уязвимостей в качестве простейшего элемента информационной безопасности как объекта моделирования, в рамках которой угрозы разделены на угрозы технологических уязвимостей и уязвимостей реализации, создающих угрозы условных технологических уязвимостей. Показано, что в качестве объекта моделирования угроз уязвимостей для последующего моделирования угрозы атаки следует рассматривать именно угрозы уязвимостей реализации, при этом моделирование может проводиться без каких-либо экспертных оценок — исключительно с использованием существующей статистики в отношении параметров безопасности угроз уязвимостей. Обоснована корректность использования для моделирования угроз атак марковских моделей с дискретными состояниями и непрерывным временем, широко применяемых в теории надежности для моделирования систем с отказами и восстановлениями. Вместе с тем, показана необходимость включения в модель угрозы уязвимости элементов схемы "гибели и размножения", ввиду возможности возникновения в системе одновременно нескольких однотипных уязвимостей, создающих одну и ту же угрозу атаки, чем задача моделирования принципиально отличается от задачи моделирования в теории надежности. Предложена интерпретация угрозы атаки схемой последовательного резервирования угроз уязвимостей, определяющая подход к моделированию угрозы атаки на информационную систему с использованием построенных моделей массового обслуживания для угроз уязвимостей. Приведен пример количественной оценки актуальности угрозы уязвимости и угрозы атаки, создаваемой одной угрозой уязвимости реализации. Этот пример иллюстрирует возможности предложенного подхода к моделированию.

Ключевые слова: *информационная система, безопасность, угроза уязвимости, угроза атаки, актуальность угрозы, марковская модель, система массового обслуживания, отказ, восстановление, характеристика безопасности*

Введение

Известными методами моделирования угроз безопасности информационных систем в качестве простейшего элемента информационной безопасности рассматривается угроза атаки на информационную систему [1—5]. Моделирование угроз атак реализуется в целях выявления актуальных угроз — угроз, от которых требуется реализация защиты. С подобным подходом к моделированию связан ряд принципиальных недостатков. Прежде всего, это необходимость экспертного задания ключевой характеристики безопасности — вероятности возникновения угрозы атаки. Экспертные оценки используются и при построении модели нарушителя [5], что опять же необходимо для оценки актуальности угрозы атаки, но уже применительно к конкретной информационной системе, для которой проектируется система защиты. При моделировании угрозы безопасности информационной системы в целом, основанном на использовании в качестве простейшего элемента информационной безопасности угрозы атаки, по понятным причинам — не анализируются составляющие угрозы атаки, создаваемой угрозами уязвимостей, угрозы атак рассматриваются в качестве независимых событий, исходя из чего, используются соответствующие расчетные формулы. Но подобный исходный посыл не корректен в принципе, так как реальные угрозы атак создаются выявляемыми в системе уязвимостями, при этом события возникновения угроз атак, как правило, зависимы по уязвимостям, поскольку многими атаками эксплуатируются одни и те же уязвимости. Например, подавляющая часть угроз атак предполагает внедрение и последующее исполнение на защищаемом компьютере вредоносной программы. Важным является и то, что оперируя при моделировании не простейшим элементом безопасности, каким является угроза уязвимости, а угрозами атак, которые крайне разнородны, невоз-

можно обосновать требования к входным параметрам модели. При проектировании же системы защиты крайне важно то, что в конечном счете системой защиты, если ее рассматривать не как некую абстракцию при моделировании, а пытаться реально спроектировать, защита от угроз атак реализуется нивелированием именно соответствующих угроз уязвимостей, создающих эти угрозы атак.

В качестве простейшего элемента безопасности информационной системы при построении математических моделей угрозы атаки на информационную систему предлагается рассматривать угрозу уязвимости, что позволяет использовать существующую и непрерывно ведущуюся статистику в отношении выявляемых и устраняемых уязвимостей при задании входных параметров разрабатываемых моделей.

1. Модели угрозы уязвимости

Под *уязвимостью* в качестве простейшего элемента безопасности информационной системы будем понимать свойство системы, создающее условие для реализации на нее атаки. В общем случае к угрозам уязвимостей информационной системы могут быть отнесены технологические недостатки ее построения, включая отсутствие требуемых функций защиты (технологическая уязвимость), а также ошибки в используемом прикладном и системном программном обеспечении, позволяющие осуществить обход реализованных функций защиты (уязвимость реализации). Угроза атаки на информационную систему в общем случае создается совокупностью угроз уязвимостей — технологических уязвимостей и уязвимостей угроз реализации, наличие (выявление) которых в системе необходимо для осуществления данной атаки.

Уточним. В любом случае атакой эксплуатируется технологическая уязвимость (уязвимости), связанная с технологическими недостатками построения системы, в части реализации ее защиты. Технологические уязвимости могут быть классифицированы — разделены; на безусловные и условные. *Безусловная технологическая уязвимость* предполагает возможность ее использования атакой без возникновения каких-либо дополнительных условий в системе. Пример безусловной технологической уязвимости — возможность исполнения на компьютере созданного файла под учетной записью интерактивного пользователя. *Условная технологическая уязвимость* возникает в системе лишь при возникновении неких дополнительных условий (без этих условий она отсутствует в системе, а ее угроза непосредственно связана с угрозой выявления соответствующей уязвимости реализации), например, выявленной соответствующей ошибки программирования в системном, либо в прикладном средстве, что уже является угрозой реализации (угрозой реализации соответствующей технологической уязвимости). Пример условной технологической уязвимости — возможность исполнения на компьютере созданного файла с системными правами. Естественно, что в штатном режиме функционирования (без возникновения соответствующих условий), это не является технологической уязвимостью — какой-либо ошибкой, либо некорректностью реализации защиты, однако при выявлении соответствующих ошибок программирования в системных средствах (рассмотрим далее), эта возможность уже может рассматриваться в качестве технологической уязвимости.

Отметим, что к условным технологическим уязвимостям (не являющимся уязвимостями без возникновения соответствующих условий) могут быть отнесены и широко используемые на практике штатные возможности современных приложений, позволяющих расширять их с использованием макросов, скриптов и т. д. Угроза данных уязвимостей связана с возможностью наделения соответствующего приложения вредоносным кодом.

Таким образом, в общем случае задача реализации защиты информационной системы (задача построения системы защиты) сводится к выявлению и нивелированию угроз безусловных и условных технологических уязвимостей. Нивелирование угроз безусловных технологических уязвимостей в том числе, может решать система защиты посредством их перевода в категорию условных, например, безусловная угроза возможности исполнения на компьютере интерактивным пользователем созданного файла переводится в категорию условных с использованием антивирусного средства защиты — угроза становится реальной при условии, если вредоносная программа, загруженная на компьютер, не детектируется соответствующим антивирусным средством защиты. Естественно, что нивелирование выявленных уязвимостей реализации (в частности, исправление ошибок в программных средствах) никак не связано с задачей системы защиты — это задача разработчика соответствующих программных средств. Отметим, что реализация защиты должна рассматриваться в отношении одной (либо в отношении их необходимых совокупностей) задач защиты информации — обеспечение конфиденциальности (защита от хищения) информации, обеспечение целостности (защита от несанкционированной модификации) и доступности информации, поскольку в общем случае угрозы уязвимостей для них различны.

Под потенциальной угрозой для информационной системы понимаем угрозу, возникновение которой потенциально возможно, под реальной угрозой — реально возникшую угрозу — в системе создаются условия для реализации атаки.

Акцентируем внимание на следующем важном моменте, который должен быть учтен при последующем моделировании. Здесь и далее, говоря об уязвимости реализации и об угрозе уязвимости реализа-

ции, в общем случае мы понимаем некую совокупность однотипных уязвимостей, создающих одни и те же условия для реализации атаки на информационную систему. Например, выявляемые ошибки в системных программных средствах, позволяющие запустить программу с системными правами, мы рассматриваем как одну уязвимость. Вместе с тем для реализации атаки на повышение привилегий можно использовать выявленные уязвимости реализации (ошибки программирования) в различных компонентах системы, работающих в режиме ядра, например, для ОС семейства Windows — это драйвер подсистемы Windows (Win32k.sys), системные драйверы (KM *drives*) и ядро *ntoskrnl* (NTOS) [6].

С точки зрения последующего моделирования важным является необходимость учета того, что в общем случае в системе одновременно может присутствовать несколько выявленных и не устраненных однотипных уязвимостей реализации.

В отношении выявляемых и исправляемых уязвимостей реализации постоянно ведется соответствующая статистика и аналитическая обработка в целях предоставления пользователям оперативной информации о выявленных уязвимостях и об уровне их критичности. На сегодняшний день наиболее широкое практическое использование нашли следующие способы классификации и количественной оценки актуальности уязвимостей: схема классификации уязвимостей NIPC; шкала анализа уязвимостей SANS; система оценки критичности уязвимостей Microsoft; система оценки уязвимостей по стандарту PCI DSS; системы US—CERT, CVSS и nCircle. Они различаются учитываемыми при классификации уязвимостей параметрами и шкалами оценки уязвимостей.

В качестве примера рассмотрим Общую систему оценки уязвимости (Common Vulnerability Scoring System, CVSS) [7]. Данная система предназначена для классификации уязвимостей по шкале критичности от 0 до 10:

- 0,0—3,9 — низкая степень;
- 4,0—6,9 — средняя степень;
- 7,0—9,9 — высокая степень;
- 10 — критическая степень.

Оценка (отнесение к уровню критичности) уязвимости проводится на основе набора показателей (вектор доступа, сложность доступа, аутентификация, влияние на конфиденциальность, влияние на целостность, влияние на доступность).

Информации в открытых источниках о выявляемых и устраняемых уязвимостях реализации достаточно много. Используя данную статистику, можно определить соответствующие стохастические параметры угрозы уязвимости — интенсивность возникновения (выявления) λ и интенсивность устранения μ, и построить соответствующую математическую модель, позволяющую определять вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости $P_{0y} = f(\lambda, \mu)$. Данная характеристика угрозы уязвимости может позиционироваться в качестве количественной оценки ее актуальности.

Заметим, что моделирование имеет смысл проводить в отношении угроз уязвимостей реализации, поскольку для угрозы безусловной технологической уязвимости $P_{0y} = 0$ (не являясь безусловными уязвимостями, а порой, создаваемые штатными возможностями программных средств, приводящих при определенных условиях к уязвимостям, на практике подобные уязвимости разработчиками не исправляются).

С учетом сказанного уровень защищенности информационной системы может быть классифицирован следующим образом. Будем говорить, что информационная система *не защищена* при наличии в ней хотя бы одной известной безусловной технологической уязвимости, позволяющей реализовать несанкционированный доступ в целях (либо с совокупностью целей, в зависимости от решаемых задач защиты) нарушения конфиденциальности, целостности, доступности информации. Система имеет *базовый уровень защищенности*, если в ней отсутствуют известные безусловные технологические уязвимости, гипотетически идеально защищена при отсутствии в ней как безусловных, так и потенциально возможных условных технологических уязвимостей. Естественно, что какое-либо проектирование системы защиты для информационной системы имеет смысл применительно к системе базового уровня защищенности, а оптимальность получаемого решения оценивается исходя из защиты от актуальных угроз атак, требующих для реализации использования условных технологических уязвимостей. Защита (дополнительно к базовой) реализуется посредством нивелирования проектируемой системой защиты актуальных угроз условных технологических уязвимостей. В результате проектирования необходимо обеспечить требуемый (актуальный) уровень безопасности защищаемой информационной системы.

Соответственно, моделирование угроз уязвимостей имеет смысл и будет далее проводиться в целях оценки актуальности, именно в отношении угроз уязвимостей реализации.

Замечание. Уязвимости реализации по своей сути разнородны. Некоторые из них при выявлении не создают реальной угрозы до тех пор, пока нарушителем не предпринято соответствующих действий, позволяющих реализовать эту угрозу, например, не создано программного средства, позволяющего осуществить атаку на выявленную уязвимость (эксплойта). Сложность использования уязвимостей соответствующего типа можно учесть, определяя параметр λ только для той части уязвимостей, которые реально эксплуатировались — для которых были разработаны и использовались эксплойты (та-

кая статистика также ведется). Например, в 2013 г., несмотря на множество выявленных, эксплуатировалась лишь одна уязвимость драйвера Win32k.sys.

В отношении угрозы уязвимости (здесь и далее, если нет соответствующего уточнения, говорим об угрозе уязвимости реализации) информационную систему необходимо рассматривать как систему с отказами и восстановлениями характеристики безопасности. Отказом здесь выступает выявление, а восстановлением — устранение выявленной уязвимости.

В теории надежности для моделирования систем с отказами и восстановлениями характеристики надежности (в данном случае ремонта) объектов, как правило, используется аппарат марковских случайных процессов при допущениях о пуассоновском характере потока заявок и о показательном распределении времени обслуживания [8]. Как известно, процесс, протекающий в физической системе, называется марковским (или процессом без последействия), если для каждого момента времени вероятность любого состояния системы в будущем зависит только от состояния системы в настоящий момент и не зависит от того, каким образом система пришла в это состояние. Проанализируем, можно ли использовать (корректно ли использование, а если корректно, то как могут интерпретироваться получаемые результаты) данный аппарат в нашем случае, т. е. для моделирования систем с отказами и восстановлениями, но уже характеристики безопасности.

С этой целью проанализируем, что собой представляют уязвимости, выявление которых в системе создает реальную угрозу атаки. Как отмечали ранее, возникновение уязвимости в информационной системе в общем случае может быть вызвано двумя причинами: отсутствием, либо некорректностью решения соответствующей задачи защиты, либо ошибками реализации средств информационной системы, например, ошибками программирования, которые могут эксплуатироваться нарушителем для обхода защиты. В качестве эксплуатационных параметров уязвимости рассматриваем интенсивность возникновения уязвимости λ, и интенсивность устранения уязвимости μ. Под возникновением уязвимости (здесь и далее) естественно понимаем ее выявление нарушителем.

Предполагая, что система содержит конечное (пусть и очень большое) число не выявленных уязвимостей, можем заключить, что в данном случае процесс не является марковским, поскольку выявление и устранение каждой уязвимости приводит к уменьшению их числа на конечном исходном множестве, т. е. имеем процесс с последействием, при этом входной поток не будет являться пуассоновским, поскольку в этих предположениях $\lambda \neq \text{const}$. Однако оценим, как будут на практике изменяться параметры уязвимости в процессе эксплуатации информационной системы. Очевидно, что в общем случае интенсивность возникновения уязвимости λ по прошествии некоторого времени будет снижаться, поскольку в первую очередь нарушитель будет выявлять наиболее простые недочеты реализации защиты и ошибки в программном обеспечении (увеличение сложности выявления уязвимости естественно приведет к снижению интенсивности λ). В отношении же параметра μ можем сказать, что он никак не связан со сложностью выявления уязвимости, определяется исключительно типом уязвимости (например, ошибки в системных драйверах и в приложениях требуют различной трудоемкости исправления), т. е. для каждого типа уязвимости можем принять $\mu = \text{const}$.

Теперь допустим, что мы спроектировали систему защиты, применив формальную экстраполяцию (прогнозная экстраполяция здесь мало применима, ввиду высокой интенсивности переходов на новые версии программных средств в современных информационных системах) с использованием марковской модели. Тем самым при моделировании мы предположили, что поток без последействия, т. е. интенсивности возникновения уязвимости λ, и устранения уязвимости μ будут неизменными в процессе последующей эксплуатации защищенной информационной системы. Очевидно, что с учетом сказанного ранее (а именно, что значение λ будет только уменьшаться, а μ останется неизменным в процессе последующей эксплуатации системы), используя подобную модель мы найдем граничные (при худших для системы условиях) значения требуемых характеристик, учет которых гарантирует, что "хуже не будет". На самом же деле, определение значений именно таких характеристик при проектировании системы защиты и требуется (не можем же мы проектировать систему защиты, оперируя заниженными, с учетом их уменьшения в процессе эксплуатации системы, значениями параметров уязвимости). Вот если бы последействие приводило к увеличению λ в процессе эксплуатации информационной системы, тогда, другое дело, подобное последействие при моделировании необходимо было бы учитывать.

Из сказанного можем сделать крайне важный вывод о том, что при моделировании угрозы уязвимости, угрозы атаки и угрозы безопасности информационной системы в целом, поскольку все угрозы (и угрозы атаки и угрозы безопасности информационной системы в целом) в конечном счете создаются угрозами уязвимостей, можно использовать марковские модели, позволяющие в данном случае определять граничные значения характеристик безопасности, которые и необходимо использовать при проектировании системы защиты. Это существенно упрощает рассматриваемую задачу моделирования.

Теперь в двух словах о прогнозировании. Используя рассмотренный подход к моделированию с использованием марковских моделей, характеристики угроз уязвимости мы оцениваем за некоторый прошедший интервал времени, в то время как система защиты проектируется для использования в будущем.

В методическом плане основным инструментом любого прогноза является схема экстраполяции [9]. Сущность экстраполяции заключается в изучении сложившихся в прошлом и настоящем устойчивых тенденций развития объекта прогноза и в переносе их на будущее.

Различают формальную и прогнозную экстраполяцию. Формальная экстраполяция базируется на предположении о сохранении в будущем прошлых и настоящих тенденций развития объекта прогноза; при прогнозной экстраполяции фактическое развитие увязывается с гипотезами о динамике исследуемого процесса с учетом изменений влияния различных факторов в перспективе.

При моделировании, задавая параметры угроз безопасности, мы пользуемся формальной экстраполяцией, исходя из прогноза о том, что в будущем, по причинам, рассмотренным выше, они хуже не станут.

С учетом того, что вероятностью одномоментного появления в системе нескольких однотипных уязвимостей (не одновременного присутствия, о чем говорили ранее) можем пренебречь, процесс возникновения и устранения в системе угрозы уязвимости может быть описан схемой "гибели и размножения" [10]. Тогда для случая одного обслуживающего прибора искомая характеристика безопасности (стационарный коэффициент готовности, в данном случае, готовности к безопасной эксплуатации в отношении угрозы уязвимости) определяется следующим образом:

$$P_{0y} = 1 - \rho, \text{ где } \rho = \lambda/\mu,$$

а вероятность наличия в системе одновременно R неустраненных уязвимостей $P_{Ry} = \rho^R(1 - \rho)$.

В качестве обслуживающего прибора в нашем случае выступает коллектив разработчиков, устраняющих выявленную в системе уязвимость с интенсивностью μ. На практике одновременно может устраняться несколько уязвимостей, т. е. в общем случае следует рассматривать схему "гибели и размножения" с C обслуживающими приборами. Для такой модели искомая характеристика определяется следующим образом:

$$P_{0y} = \left(1 + \rho + \frac{\rho^2}{2!} + \ldots + \frac{\rho^C}{C!}\right)^{-1},$$

а вероятность наличия в системе одновременно R неустраненных уязвимостей $P_{Ry} = \frac{\rho^C}{C!} P_{0y}$.

Можно предположить, что при условии $\rho = \frac{\lambda}{\mu} \ll 1$ значение вероятности $P_{R>1y}$ мало и им можно пренебречь, что далее упростит построение модели. Возможность упрощения модели имеет смысл исследовать, ввиду того, что нам далее потребуется построить модели угрозы атаки и модели угрозы безопасности информационной системы в целом, в которых угроза уязвимости выступает простейшим элементом безопасности. Оценим данное условие, для чего рассмотрим изменение на интересующих нас интервалах значений характеристик P_{Ry} от изменения значений характеристики ρ для одноканальной (табл. 1) и двухканальной ($C = 2$) (табл. 2) систем.

Проанализировав результаты, представленные в табл. 1 и в табл. 2, можем сделать следующие выводы. Если $\rho \leqslant 0{,}2$ при моделировании угрозы уязвимости можно использовать одноканальную схему "гибели и размножения", если $\rho > 0{,}2$ необходимо использовать двухканальную схему.

Замечание. Условие $\rho > 0{,}9$ для угрозы уязвимости реализации не анализируется, поскольку при выполнении данного условия можно принять $P_{0y} = 1$, отнеся соответствующую условную технологическую уязвимость к безусловным, а информационную систему — к незащищенным.

К слову сказать, приведенные в табл. 2 результаты исследования позволяют оценить современное положение дел в области информационной безопасности. Так, при средней продолжительности устранения уязвимостей, составляющей 30 дней (некоторые уязвимости в современных ОС устраняются месяцами), выявление всего лишь шести уязвимостей в год обеспечивает значение коэффициента готовности, близкое к 0,5.

Таблица 1

Характеристики одноканальной системы

P_{Ry}	ρ				
	0,1	0,2	0,3	0,4	0,5
P_{0y}	0,90	0,80	0,70	0,60	0,50
P_{1y}	0,09	0,16	0,21	0,24	0,25
$P_{R \geqslant 2y}$	0,01	0,04	0,09	0,16	0,25

Таблица 2

Характеристики двухканальной системы

P_{Ry}	ρ						
	0,3	0,4	0,5	0,6	0,7	0,8	0,9
P_{0y}	0,74	0,68	0,60	0,56	0,51	0,47	0,43
P_{1y}	0,23	0,27	0,32	0,34	0,36	0,38	0,39
P_{2y}	0,03	0,05	0,08	0,10	0,13	0,15	0,18
$P_{R \geqslant 3y}$	0	0	0	0	0	0	0

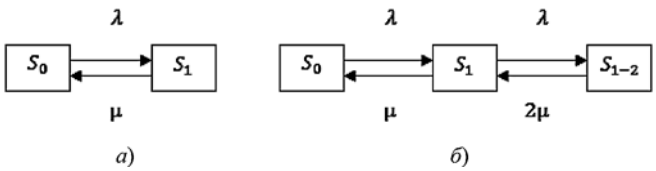

Рис. 1. Графы системы состояний случайного процесса для угрозы уязвимости:
а — при $\rho < 0{,}2$; *б* — при $\rho > 0{,}2$

Графы состояний случайного процесса выявления и устранения уязвимостей (марковского процесса с дискретными состояниями и непрерывным временем), которые нами далее будут использованы, представлены на рис. 1, где S_0 — исходное состояние системы, S_1 — в системе выявлена и не устранена одна из уязвимостей, S_{1-2} — в системе выявлены и не устранены две уязвимости.

2. Интерпретация угрозы атаки на информационную систему

В общем случае реализация атаки предполагает использование нескольких присутствующих в системе уязвимостей, причем, как правило, в определенной последовательности. В работе [1] угрозу атаки на информационную систему было предложено представлять соответствующим орграфом, проиллюстрированным на рис. 2, *а*, где через P_{0yr}, $r = 1, ..., R$, обозначается вероятность отсутствия в системе r-й уязвимости (информационная система готова к безопасной эксплуатации в отношении угрозы r-й уязвимости) — одной из R угроз уязвимостей, последовательно (дуги графа определяют последовательность использования выявленных уязвимостей при реализации атаки) используемых атакой на информационную систему.

При подобном представлении угроза атаки на информационную систему может интерпретироваться схемой параллельного резервирования угроз уязвимостей (в общем случае безусловных и условных технологических уязвимостей и уязвимостей реализации), резервируемыми и резервирующими элементами которой являются угрозы уязвимости

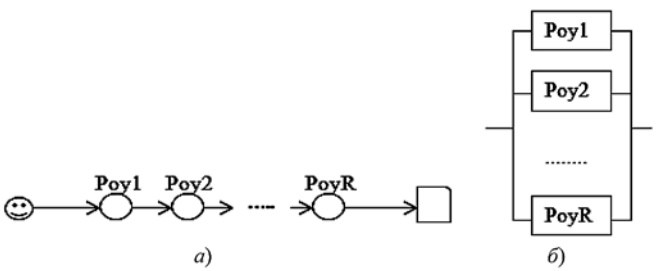

Рис. 2. Орграф угрозы атаки и ее интерпретация схемой параллельного резервирования угроз уязвимостей:
а — орграф угрозы атаки; *б* — схема параллельного резервирования

(рис. 2, *б*), поскольку каждая угроза уязвимости, присутствующая в системе с вероятностью P_{0yr}, может рассматриваться в качестве резервирующего элемента (с вероятностью P_{0yr} предотвращает атаку).

Замечание. Для угроз технологических уязвимостей как для безусловных, так и для условных имеем $P_{0yr} = 1$, для угроз уязвимостей реализации значения характеристики P_{0yr} необходимо рассчитывать с использованием представленных выше моделей.

Исключив из орграфа угрозы атаки вершины угроз технологических уязвимостей, для которых $P_{0yr} = 1$, получим орграф угроз уязвимостей реализации и можем определить характеристику — вероятность того, что информационная система готова к безопасной эксплуатации в отношении угрозы атаки P_{0a} (очевидно, что события выявления и устранения уязвимостей реализации, эксплуатируемых атакой, можно рассматривать в качестве независимых), в предположении, что все R угроз уязвимостей, оставшихся на приведенном орграфе, — это угрозы уязвимостей реализации [1]:

$$P_{0a} = 1 - \prod_{r=1}^{R} (1 - P_{0yr}).$$

Данная характеристика угрозы атаки может позиционироваться в качестве количественной оценки ее актуальности [1] для реализации защиты.

Данная интерпретация позволяет представлять систему защиты информационной системы (СЗИ) в виде отдельной вершины (отдельных вершин) на орграфе угрозы атаки с параметрами $\lambda_{СЗИ}$ и $\mu_{СЗИ}$ уже собственно системы защиты (это параметры угроз уязвимостей системы защиты, куда включены и безусловные, и условные угрозы технологических уязвимостей). При этом можно сделать вывод о том, что угрозы технологических уязвимостей, создающие угрозу атаки, с точки зрения их нивелирования системой защиты, эквивалентны [1], поскольку при нивелировании любой из них угрозы системы защиты включаются в схему параллельного резерва (см. рис. 1, *б*) одинаково, с параметрами безопасности системы защиты: $\lambda_{СЗИ}$ и $\mu_{СЗИ}$.

Если обозначить вероятность того, что система защиты, используемая для нивелирования одной из угроз технологических уязвимостей, создающих угрозу атаки, готова к безопасной эксплуатации, через $P_{0СЗИ}$, то вероятность того, что защищенная в отношении угрозы уязвимости информационная система будет готова к безопасной эксплуатации ($P_{0УЗИС}$) при использовании системы защиты, нивелирующей эту уязвимость, может быть определена следующим образом:

$$P_{0УЗИС} = 1 - (1 - P_{0y})(1 - P_{0СЗИ}).$$

Вероятность того, что защищенная информационная система готова к безопасной эксплуатации ($P_{0АЗИС}$) в отношении угрозы атаки, при использовании сис-

темы защиты, нивелирующей одну из угроз технологических уязвимостей, создающих угрозу атаки, равна $P_{0\text{АЗИС}} = 1 - (1 - P_{0\text{СЗИ}}) \prod_{r=1}^{R} (1 - P_{0yr})$.

В двух словах остановимся на вопросах нивелирования угрозы технологической уязвимости системой защиты. Например, возможность, в том числе и с системными правами, исполнения в системе создаваемых в процессе работы интерактивными пользователями файлов, можно рассматривать в качестве технологической уязвимости системы. Сегодня на практике широко распространены решения, не предполагающие нивелирования (устранения) угроз технологических уязвимостей, предполагающие перевод угроз безусловных технологических уязвимостей в группу угроз условных уязвимостей за счет создания системой защиты дополнительных условий возможности их реализации. К подобным решениям можно, например, отнести антивирусные средства защиты, основанные на анализе контролируемых событий на соответствие неким эталонным множествам (например, сигнатурный и/или поведенческий анализ). Поскольку данные эталонные множества априори не могут быть полными, не может быть полностью (здесь не рассматриваются угрозы уязвимости реализации) и нивелирована угроза безусловной технологической уязвимости запуска создаваемых исполняемых файлов. В результате этого значение параметра $\lambda_{\text{СЗИ}}$ подобных систем защиты растет по мере увеличения интенсивности создаваемых вредоносных программ (функционально зависит от интенсивности создания новых вредоносных программ). По самым оптимистичным прогнозам современными антивирусными средствами защиты выявляется — детектируется, до 75 % новых вредоносных программ (например, в отношении новых технологий детектирования, опирающихся на возможности KSN-(технология Kaspersky Security Network, основанная на создании антивирусного облака), утверждается, что их применение позволило увеличить с 60 до 75 % долю угроз, обнаруживаемых эвристическими методами без обновления классических антивирусных баз, т. е. 25 % угроз средством защиты не детектируются, а интенсивность создания новых вредоносных программ определяется десятками [11], если уже не сотнями миллионов в год. С учетом сказанного несложно рассчитать $\lambda_{\text{СЗИ}}$ подобных современных систем защиты. Задавая различные расчетные значения $\mu_{\text{СЗИ}}$ (а это, по крайней мере, единицы, а то и десятки дней, ведь мы говорим о тех вредоносных программах, которые не выявляются антивирусным средством — их еще нужно каким-то образом обнаружить), можно легко определить сколько обслуживающих приборов (в данном случае одновременно работающих над различными сигнатурами вирусных аналитиков C) потребуется антивирусной компании для выполнения требования к стационарности системы: $\frac{\lambda_{\text{СЗИ}}}{C_{\mu_{\text{СЗИ}}}} < 1$. К слову сказать, из этого анализа можем сделать вывод о том, что основными характеристиками эффективности антивирусной системы защиты является не интенсивность выявления сигнатуры вируса $\mu_{\text{СЗИ}}$, а средняя длина очереди заявок на облуживание (выявленных вредоносных программ) и среднее время пребывания заявки на обслуживание в очереди. Отдельно стоит задача оценки выявления вредоносной программы, не детектируемой антивирусным средством защиты. Отметим, что для моделирования подобных систем марковские процессы уже не применимы, поскольку интенсивность создания новых вредоносных программ (что и не удивительно при такой эффективности защиты) растет из года в год, причем крайне стремительно [11].

Оценим потенциальные возможности реализации эффективной защиты с использованием систем защиты, нивелирующих угрозы технологических уязвимостей, основанных на реализации разграничительной политики доступа к ресурсам [12], в частности, эффективное решение защиты от вредоносных программ, призванное нивелировать угрозу соответствующей уязвимости, рассмотрено в работе [13]. С этой целью получим и проанализируем значения характеристики P_{0y} средства защиты $P_{0\text{УСЗИ}}$ при различных значениях $\lambda_{\text{СЗИ}}$ и $\mu_{\text{СЗИ}}$ (поскольку нас интересует условие $\rho \leqslant 0{,}2$, то для расчетов используем модель, приведенную на рис. 1, *а*). Например, $P_{0\text{УСЗИ}} = 0{,}99$ достигается при выявлении в средстве защиты только одной уязвимости в год при продолжительности ее устранения 3,65 дня. При выявлении двух уязвимостей в год при той же продолжительности их устранения, уже имеем $P_{0\text{УСЗИ}} = 0{,}98$, этот же результат получим при выявлении в средстве защиты одной уязвимости в год при продолжительности ее устранения, составляющей 7,3 дня.

Отметим, что соответствующие требования к характеристикам системы защиты могут задаваться (и на практике задаются) в задании на их техническое сопровождение, их выполнение при этом легко проконтролировать. К слову сказать, из практического опыта можем заключить, что, естественно, без каких-либо расчетов, интуитивно на практике задаются требования к значению характеристики системы защиты $P_{0\text{УСЗИ}}$ не ниже 0,9 (если это, конечно, не системы антивирусной защиты).

Из проведенного исследования можно сделать вывод о том, что потенциально высокое значение (0,9 и выше) коэффициента готовности системы защиты к безопасной эксплуатации систем защиты, решающих задачу нивелирования угроз технологических уязвимостей, достижимо.

Акцентируем внимание на следующем принципиальном моменте. Методы контроля и разграничения прав доступа, используемые для реализации разграничительной политики доступа к ресурсам, составляющие основу практически любой современной системы защиты информации (не говорим здесь о методах, основанных на анализе контролируемых событий на соответствие соответствующим эталонным множествам), служат на практике для разделения между пользователями компьютерных ресурсов с учетом решаемых ими задач в информационной системе.

В данной работе сформулирована принципиально иная постановка задачи защиты, для решения которой могут и, как мы выше показали, должны применяться методы контроля и разграничения прав доступа, — задача нивелирования безусловных и условных технологических уязвимостей, решаемая в целях защиты от актуальных угроз атак для повышения уровня безопасности информационной системы. Естественно, что данная задача защиты, иная собственно в своей постановке, требует и принципиально иных решений, в том числе технических, для реализации разграничительной политики доступа к ресурсам, создаваемой уже совершенно с иными целями. Требования к методам контроля и разграничения прав доступа, используемым для решения данной задачи защиты, реализация которых позволяет построить безопасную систему, собственно методы и их практическая реализация на примере апробированных технических решений, разграничительные политики доступа, используемые для защиты от наиболее актуальных современных угроз атак, рассмотрены в работе [12].

3. Пример количественной оценки актуальности угрозы уязвимости и угрозы атаки

В качестве примера рассмотрим угрозу атаки на повышение привилегий. Для исследования она интересна тем, что экспертная оценка ее актуальности при проектировании системы защиты совсем не очевидна. Подобная угроза атаки предполагает внедрение на компьютер вредоносной программы, что можно рассматривать как безусловную технологическую уязвимость, использование выявленной уязвимости реализации (выявленной программной ошибки) в компоненте (программе) ядра ОС, запущенного с системными правами, для исполнения внедренного на компьютер в процессе работы исполняемого вредоносного файла, что можно рассматривать уже в качестве условной технологической уязвимости системы (возможно при выявлении соответствующей ошибки в системном средстве), с системными правами. Получаем орграф угрозы атаки, предполагающей последовательное использование нарушителем данных трех уязвимостей (орграф угрозы атаки содержит в своем составе три взвешенных вершины). Если возможность загрузки на компьютер исполняемого файла и возможность исполнения созданного в процессе работы системы файла, как отмечали, можно отнести к уязвимостям технологического характера (они всегда присутствуют в незащищенной системе) — для них $P_{0yr} = 1$, то интересующую нас угрозу уязвимости реализации — уязвимости, возникающей в результате выявления программных ошибок в компонентах (программах) ядра ОС, можно промоделировать с использованием соответствующей статистики.

Заметим, что чтобы дать экспертную оценку актуальности угрозы данной атаки, можно, например, воспользоваться исследованиями, представленными в работах [14, 15], результаты которых приведены на рис. 3 и 4 (см. четвертую сторону обложки).

Как дать экспертную (хотя бы качественную, не говоря уже о количественной) оценку актуальности угрозы рассматриваемой атаки, исходя из подобной статистики, а уж тем более, как ее обосновать? Насколько адекватной будет подобная оценка?

Построим математическую модель исследуемой угрозы уязвимости реализации, для чего обратимся к соответствующей статистике, приведенной в работе [16]. Выявленные и исправленные за 2014 г. уязвимости уровня ядра ОС Windows сведены в табл. 3.

Как видим из табл. 3, уязвимостей, позволяющих осуществить атаку на повышение привилегий (Elevation of Privilege) за 2014 г. было выявлено достаточно много. Однако уязвимости уровня ядра ОС сложны в практическом использовании для реализации соответствующей атаки, так как требуют разработки соответствующего эксплойта. Уязвимости, для которых были созданы и использованы эксплойты, в табл. 3 подчеркнуты. Что же касается угрозы атак на повышение привилегий, то за 2014 г. были созданы эксплойты к следующим трем уязвимостям: CVE-2014-6324, CVE-2014-4113, CVE-2014-0318 (примем для расчетов значение интенсивности выявления угрозы интересующей нас уязвимости — 3 в год).

Исходя из того, что среднее время устранения выявленных уязвимостей в ОС Windows составляет около месяца [17] (примем значение интенсивности устранения выявленной уязвимости — 12 в год), можем оценить загрузку соответствующей системы массового обслуживания, $\rho = 0{,}25$. С учетом сказанного ранее получаем количественную оценку актуальности угрозы рассматриваемой уязвимости $P_{0y} = 0{,}75$, используя которую, можно утверждать, что в любой момент времени вероятность того, что в системе угроза уязвимости реализации, позволяющая реализовать атаку на повышение привилегий, реальна (уязвимость присутствует), составляет 25 %. Заметим, что таким же значением будет характеризоваться и уровень актуальности угрозы атаки на повышение привилегий, поскольку для

Таблица 3

Исправленные уязвимости для различных компонентов Windows

Компонент	Обновление	Тип	Уязвимость
Windows UMC (VBScript, Direct2D, MSXML, DirectShow, SAMR, File Handling/ kernel32.dll, Shell handler/ shell32.dll, Remote Desktop, Journal, On-Screen Keyboard, Media center/mcplayer. dll, Installer, Task Scheduler, OLE, Message Queuing, Schannel, Kerberos, Audio Service, IIS, IME (Japanese), GDI+/gdi32.dll, RPC/rpcrt4.dll, Graphics/ windowscodecs.dll	MS14-011, MS14-007, MS14-005, MS14-013, MS14-016, MS14-027, MS14-030, MS14-033, MS14-038, MS14-039, MS14-041, MS14-043, MS14-049, MS14-054, MS14-060, MS14-062, MS14-064, MS14-066, MS14-067, MS14-068, MS14-071, MS14-074, MS14-076, MS14-078, MS14-036, MS14-047, MS14-084, MS14-085	Remote Code Execution(11), Information Disclosure(3), Security Feature Bypass(4), Elevation of Privilege(9), Tampering(1)	CVE-2014-0271, CVE-2014-0263, ***CVE-2014-0266***, CVE-2014-0301, CVE-2014-0317, CVE-2014-0315, ***CVE-2014-1807***, CVE-2014-1816, CVE-2014-0296, CVE-2014-1824, CVE-2014-2781, CVE-2014-2780, CVE-2014-4060, CVE-2014-1814, CVE-2014-4074, CVE-2014-4114, CVE-2014-4971, CVE-2014-6332, ***CVE-2014-6352***, CVE-2014-6321, CVE-2014-4118, ***CVE-2014-6324***, CVE-2014-6322, CVE-2014-6318, CVE-2014-4078, CVE-2014-4077, CVE-2014-1818, CVE-2014-0316, CVE-2014-6363, CVE-2014-6355
Win32k	MS14-003, MS14-015, MS14-045, MS14-058, MS14-079	Elevation of Privilege(4), Denial of Service(1)	CVE-2014-0262, CVE-2014-0300, CVE-2014-0323, CVE-2014-0318, CVE-2014-1819, ***CVE-2014-4113***, ***CVE-2014-4148***, CVE-2014-6317
KM drivers (ndproxy.sys, tcpip. sys, afd.sys, fastfat. sys)	MS14-002, MS14-006, MS14-031, MS14-040, MS14-045, MS14-063, MS14-070	Elevation of Privilege(5), Denial of Service(2)	***CVE-2013-5065***, CVE-2014-0254, CVE-2014-1811, CVE-2014-1767, CVE-2014-4064, CVE-2014-4115, CVE-2014-4076
.NET Framework	MS14-009, MS14-026, MS14-046, MS14-053, MS14-057, MS14-072	Elevation of Privilege(3), Security Feature Bypass(1), Denial of Service(1), Remote Code Execution(1)	CVE-2014-0253, CVE-2014-0257, ***CVE-2014-0295 (ASLR Bypass)***, CVE-2014-1806, CVE-2014-4062 (ASLR Bypass), CVE-2014-4072, CVE-2014-4073, CVE-2014-4121, CVE-2014-4122 (ASLR Bypass), CVE-2014-4149

остальных угроз уязвимостей, создающих рассматриваемую угрозу атаки, имеем $P_{0yr} = 1$.

В порядке замечания отметим, что, как видим, по уровню актуальности данная угроза уязвимости сопоставима с актуальностью угрозы условной технологической уязвимости запуска на защищаемом антивирусной системой защиты компьютере (переводит соответствующую угрозу безусловной технологической уязвимости в категорию условных) вредоносной программы.

Для практической оценки актуальности уязвимости более наглядно и на практике целесообразно использование иной характеристики безопасности — среднего времени наработки на отказ безопасности (рассматриваем систему с отказами и восстановлениями характеристики безопасности), или среднего интервала времени между выявлениями (средняя продолжительность устранения уязвимости составляет $1/\mu$) в информационной системе уязвимости, $T_{0y} = 1/\lambda$.

Используя данную характеристику безопасности, можем заключить, что в среднем рассматриваемая угроза уязвимости, а соответственно, и угроза атаки на повышение привилегий, будет реальной каждые четыре месяца, причем нарушитель сможет ею воспользоваться в течение месяца.

Исходя из сказанного, применительно к рассматриваемому примеру можно утверждать, что без использования каких-либо дополнительных средств защиты, нивелирующих соответствующую угрозу технологической уязвимости (либо угрозу установки на компьютер исполняемого файла, либо угрозу его исполнения с системными правами), при условии соответствующей заинтересованности нарушителя в осуществлении несанкционированного доступа к обрабатываемой в системе информации (в предположении, что он реализует первую же реальную угрозу данной уязвимости), в среднем, соответствующая успешная атака будет осуществлена в течение 4—5 месяцев эксплуатации системы. А с учетом того, что речь идет о возможности запуска в системе произвольной вредоносной программы с системными правами, то эта атака может быть осуществлена нарушителем практически с любой целью.

Замечание. Решение по реализации эффективной защиты от подобных атак приведено в работе [6].

Вот она реальная количественная оценка актуальности угрозы уязвимости, получение которой не потребовало проведения экспертных оценок. Имея подобную оценку уже несложно сделать объективный вывод о том, стоит ли нивелировать по-

добную угрозу технологической уязвимости системой защиты, актуальна ли она.

Аналогичное исследование можно провести в отношении угроз уязвимостей как в системных средствах, так и в приложениях. Например, для браузера Internet Explorer за 2014 г. выявлены десятки уязвимостей, подавляющая часть из которых позволяет удаленно выполнить вредоносный код (Remote Code Execution), для семи из них были созданы соответствующие эксплойты [16].

Решение по реализации эффективной защиты от подобных атак приведено в работе [18].

Отметим, что при построении современных систем защиты информации, одной из наиболее актуальных современных задач, что наглядно иллюстрирует проведенное в работе исследование, является задача нивелирования актуальных угроз технологических уязвимостей как в системных средствах, так и в приложениях, в том числе связанных с их программной реализацией. Естественно, что для решения новой в своей постановке задачи защиты информации необходимы и новые технические решения. Так, например, подходы к защите, описанные в работах [6, 18], основаны на реализации запатентованного авторами апробированного технического решения [19].

Заключение

В данной работе исследовались вопросы моделирования и оценки актуальности угроз уязвимостей. При моделировании же угрозы атаки практический интерес представляет не только построение модели с отказами и восстановлениями характеристики безопасности, причем с учетом того, что угроза атаки создается не одной, а в общем случае некоторой совокупностью разнородных угроз уязвимостей, т. е. модели, позволяющей получать количественные оценки характеристик возникновения и устранения в системе реальной угрозы атаки, но и построение модели с фатальным отказом, предполагающей уже непосредственно реализацию нарушителем реальной угрозы атаки на конкретную информационную систему (реализацию несанкционированного доступа), для которой проектируется система защиты. С этой целью уже необходимо оценить (опять же без применения экспертных оценок в модели нарушителя) готовность реализации атаки определенной сложности нарушителем на конкретную информационную систему, характеризующую меру его заинтересованности в осуществлении подобной атаки, что в том числе предполагает количественную оценку сложности реализации атаки. Разработанные модели угрозы атаки и нарушителя будут рассмотрены во второй части статьи.

Список литературы

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

2. **Росенко А. П.** Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование. М.: Красанд, 2010.

3. **Корт С. С.** Теоретические основы защиты информации: учеб. пособие. М.: Гелиос АРВ, 2004.

4. **Корченко А. Г.** Построение систем защиты информации на нечетких множествах. Теория и практические решения. Киев: МК-Пресс, 2006.

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

6. **Щеглов К. А., Щеглов А. Ю.** Защита от атак на повышение привилегий // Вестник компьютерных и информационных технологий. 2015. № 1. С. 36—42.

7. **Полное** руководство по общему стандарту оценки уязвимостей версии 2. Часть первая. Группы метрик [Электронный ресурс]. URL: http://www.securitylab.ru/analytics/355336.php, свободный (10.01.2015).

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

9. **Саркисян В. А., Каспин В. И., Лисичкин В. А., Минаев Э. С., Пасенчник Г. С.** Теория прогнозирования и принятия решений. М.: Высшая школа. 1977.

10. **Саати Т.** Элементы теории массового обслуживания и ее приложения. М.: Советское радио, 1965.

11. **Эксперты:** трояны по-прежнему остаются самым популярным вредоносным ПО [Электронный ресурс]. URL: http://www.itsec.ru/newstext.php?news_id=100297, свободный (10.01.2015).

12. **Щеглов А. Ю.** Модели, методы и средства контроля доступа к ресурсам вычислительных систем: учеб. пособие. СПб.: Изд-во университета ИТМО, 2014. 95 с.

13. **Щеглов К. А., Щеглов А. Ю.** Система защиты от запуска вредоносных программ // Вестник компьютерных и информационных технологий. 2013. № 5. С. 38—43.

14. **Отчет** по уязвимостям 20.02—26.02 [Электронный ресурс]. URL: http://www.securitylab.ru/vulnerability/reports/420676.php, свободный (10.01.2015).

15. **Отчет** по уязвимостям за второй квартал 2008 года [Электронный ресурс]. URL: /http://www.securitylab.ru/analytics/358113.php,, свободный (10.01.2015).

16. **Windows** Exploitationin 2014. [Электронный ресурс] // URL: http://www.welivesecurity.com/wp-content/uploads/2015/01/Windows-Exploitation-in-2014.pdf, свободный (10.01.2015).

17. **"Критические** дни": Linux, Mac OS X, Solaris and Windows. [Электронный ресурс]. URL:/ http://www.securitylab.ru/opinion/297876.php, свободный (10.01.2015).

18. **Щеглов К. А., Щеглов А. Ю.** Технология изолированной обработки данных критичными приложениями // Вопросы защиты информации. 2015. Вып. 108. № 1. С. 15—22.

19. **Щеглов А. Ю., Щеглов К. А.** Система контроля доступа к файлам на основе их автоматической разметки. Патент на изобретение № 2524566. Приоритет от 18.03.2013, опубл. 27.07.2014, Бюл. № 21.

K. A. Shcheglov, Graduate Student, **A. Yu. Shcheglov,** Professor, e-mail: info@npp-itb.spb.ru
ITMO Univercity, St. Petersburg, Russian Federation

Informational System Attack Threat Modeling and Interpretation. Part 1. Vulnerability Threat Modeling and Attack Threat Interpretation

We introduce vulnerability threats classification as a basic informational security element (modeling object) in borders of which threats are divided to technological and implementation ones (which create threats of technological vulnerabilities). We show that implementation vulnerability threats must be researched as vulnerability threats modeling object (for attack modeling). While this modeling can be done without any expert assessments, i.e. just by solely using existing statistics about security parameters of vulnerabilities threats. We substantiate Markov models with discrete states and continuous time (widely used in reliability theory for modeling of systems failures and recoveries) usage correctness to model attack threats. However, we show the necessity of inclusion into vulnerability threat model of "birth and death" scheme elements (because of same time similar vulnerability possibility which create the same threat of attack). This produces fundamentally differences from the modeling problems of reliability theory. We suggest vulnerability threat serial reservation scheme as an attack threat interpretation (which defines informational system attack threat modeling approach with use of built queuing models). We show an example of vulnerability and attack threats quantitative relevance assessment (produced by single implementation vulnerability threat) illustarting possibilities of the proposed modeling approach.

Keywords: *informational system, security, vulnerability threat, attack threat, threat relevance, Markov model, queuing system, failure, recovery, security characteristics*

References

1. **Shcheglov K. A., Shcheglov A. Ju.** Matematicheskie modeli jekspluatacionnoj informacionnoj bezopasnosti, *Voprosy zashhity informacii*, 2014, Issue 106, no. 3, pp. 52—65.

2. **Rosenko A. P.** *Vnutrennie ugrozy bezopasnosti konfidencial'noj informacii: Metoodologija i teoreticheskoe issledovanie*, Moscow: Krasand, 2010.

3. **Kort S. S.** *Teoreticheskie osnovy zashhity informacii:* Uchebnoe posobie, Moscow, Gelios ARV, 2004.

4. **Korchenko A. G.** Postroenie sistem zashhity informacii na nechetkih mnozhestvah. Teorija i prakticheskie reshenija, Kiev, MK-Press, 2006.

5. **Belov E. B., Los V. P., Meshheriakov R. V., Shelupanov A. A.,** *Osnovy informacionnoj bezopasnosti,* Moscow, Gorjachaja linija — Telekom, 2006.

6. **Shcheglov K. A., Shcheglov A. Ju.** Zashhita ot atak na povyshenie privilegij, *Vestnik komp'juternyh i informacionnyh tehnologij*, 2015, no. 1, pp. 36—42.

7. ***Polnoe*** *rukovodstvo po obshhemu standartu ocenki ujazvimostej versii 2.* Chast' pervaja. Gruppy metrik [Jelektronnyj resurs]. URL: http:// www.securitylab.ru/analytics/355336.php. svobodnyj (10.01.2015).

8. **Polovko A. M., Gurov S. V.** *Osnovy teorii nadezhnosti.* — SPb.: BHV-Peterburg. — 2006.

9. **Sarkisjan V. A., Kaspin V. I., Lisichkin V. A., Minaev Je. S., Pasenchnik G. S.** *Teorija prognozirovanija i prinjatija reshenij*, Moscow, Vysshaja shkola, 1977.

10. **Saati T.** Jelementy teorii massovogo obsluzhivanija i ee prilozhenija, Moscow, Sovetskoe radio, 1965.

11. **Jeksperty:** trojany po-prezhnemu ostajutsja samym populjarnym vredonosnym PO [Jelektrorihyj resurs]. Rezhim dostupa: http://www.itsec.ru/newstext.php?news_id=100297, svobodnyj (10.01.2015).

12. **Shcheglov A. Ju.** *Modeli, metody i sredstva kontrolja dostupa k resursam vychislitel'nyh sistem*, Uchebnoe posobie, Sankt-Peterburg: Universitet ITMO, 2014.

13. **Shcheglov K. A., Shcheglov A. Ju.** Sistema zashhity ot zapuska vredonosnyh programm, *Vestnik komp'juternyh i informacionnyh tehnologij,* 2013, no. 5, pp. 38—43.

14. ***Otchet*** *po ujazvimostjam* 20.02—26.02 [Jelektronnyj resurs], URL: http://www.securitylab.ru/vulnerability/reports/420676.php, svobodnyj (10.01.2015).

15. ***Otchet*** *po ujazvimostjam za vtoroj kvartal 2008 goda* [Jelektronnyj resurs], URL: http://www.securitylab.ru/analytics/358113.php, svobodnyj (10.01.2015).

16. **Windows** Exploitationin 2014. [Jelektronnyj resurs], URL: http://www.welivesecurity.com/wp-content/uploads/2015/01/Windows-Exploitation-in-2014.pdf, svobodnyj (10.01.2015).

17. ***"Kriticheskie*** *dni": Linux, Mac OS X, Solaris and Windows,* [Jelektronnyj resurs], URL: http://www.securitylab.ru/opinion/297876.php, svobodnyj (10.01.2015).

18. **Shcheglov K. A., Shcheglov A. Ju.** Tehnologija izolirovannoj obrabotki dannyh kritichnymi prilozhenijami, *Voprosy zashhity informacii,* 2015, Issue 108, no. 1, pp. 15—22.

19. **Shcheglov A. Ju., Shcheglov K. A.** Sistema kontrolja dostupa к fajlam na osnove ih avtomaticheskoj razmetki. *Patent na izobretenie № 2524566.* Prioritet ot 18.03.2013, opubl. 27.07.2014, Bjul. № 21.