8. *Zakharov A.I., Bryakalov G.A., Chmykhova Ya.V.* Metodika otsenki vozmozhnostey vychislitel'nykh sredstv tsentra obrabotki dannykh // Vestnik Rossiyskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 1. S. 124–129.
*9. Nechay A.A., Kop'ev A.I.* Metod upravlyaemogo raspredeleniya resursov mezhdu yadrami protsessora // Vestnik Rossiyskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2018. Vyp. 2. S. 101–107.
10. *Shirobokov V.V., Nechay A.A.* Algoritm planirovaniya energosberegayushchey parallel'noy obrabotki informatsii s uchetom informatsionnoy vazhnosti i vremeni postupleniya zadach // Vestnik Rossiyskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2017. Vyp. 1. S. 88–93.

DOI: 10.25586/RNU.V9187.19.02.P.119 УДК 004.056.5

Г.И. Спиридонов

# АНАЛИЗ СУЩЕСТВУЮЩИХ И ПЕРСПЕКТИВНЫХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривается и анализируется возможная совокупность различных систем, обеспечивающих информационную безопасность предприятия, представляющего собой аппаратно-программный комплекс.
*Ключевые слова:* информационная безопасность, безопасность информационных технологий, информационные системы, перспективные методы защиты информации.

G.I. Spiridonov

# ANALYSIS OF EXISTING AND PROSPECTIVE METHODS OF INFORMATION SECURITY

The article discusses and analyzes the possible combination of various systems that ensure the information security of the enterprise, which is a hardware-software complex.
*Keywords:* information security, information technology security, information systems, prospective methods of information security.

Создание системы защиты информации может включать две дополняющие друг друга задачи – проектирование системы защиты информации, то есть ее синтез, и оценку созданной системы информационной безопасности в разрезе выполнения необходимых функций. Последняя задача обычно решается путем определения количественных характеристик соответствия комплексу требований, предъявляемых для рассматриваемой системы. В настоящее время данная задача решается единственным способом, а именно путем сертификации методов защиты информации и анализа комплекса системы защиты информации на предмет ее соответствия необходимым сертификатам.

Рассмотрим основное содержание представленных методов защиты информации, которые составляют основу механизмов защиты (рис. 1).

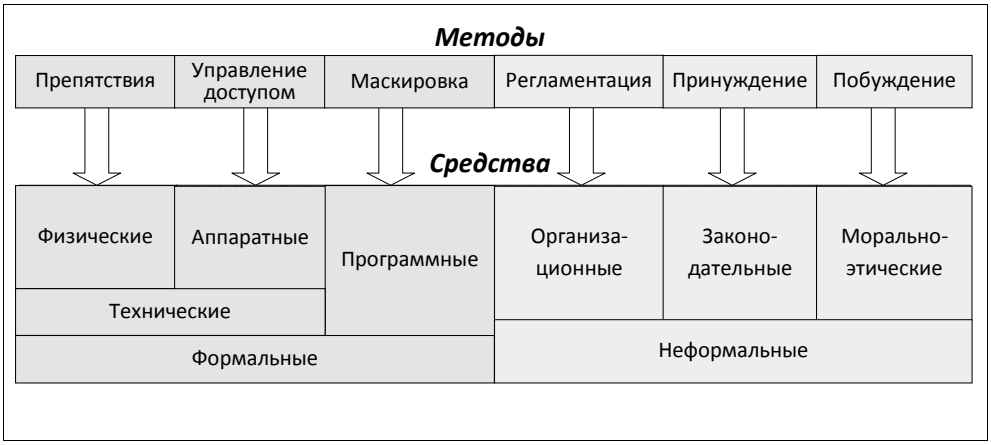


**Рис. 1.** Методы и средства обеспечения безопасности информации

Методы обеспечения безопасности информации в информационных системах (ИС):

- препятствие;
- управление доступом;
- механизмы шифрования;
- противодействие атакам вредоносных программ;
- регламентация;
- принуждение;
- побуждение.

Под препятствием понимаются методы физического преграждения дороги несанкционированному пользователю к информации, которая должна быть защищена.

*Организационные меры по обеспечению информационной безопасности* являются основной всех мероприятий по построению системы защиты информации. От того, насколько полно и качественно руководством предприятия построена организационная работа по защите информации, зависит эффективность системы защиты информации в целом, так как правильная постановка задачи на обеспечение мер по защите информации и грамотное распределение обязанностей между исполнителями – это фундамент построения любой системы.

Место и роль организационных мероприятий в общей системе используемых методов защиты конфиденциальной информации предприятия определяются важностью принятия топ-менеджментом своевременных и взвешенных решений на основании текущей ситуации с защитой информации, в том числе в результате анализа имеющихся в распоряжении предприятия методов и средств обеспечения информационной безопасности с использованием текущего пакета законодательных актов.

Грамотная реализация политики информационной безопасности современного промышленного предприятия предполагает применение комплексного подхода.

*Физические средства защиты* основаны на взаимосвязанном применении различных механических, электронных или электромеханических приспособлений, которые созда-

ны специально для создания препятствий различного рода на возможных путях несанкционированного проникновения нарушителей к самой системе или ее компонентам. Также сюда относят средства видеонаблюдения и охранную сигнализацию (рис. 2).


**Рис. 2.** Физические системы защиты

Аппаратно-программные (технические) меры для защиты обычно создаются на основе различных электронных устройств в совокупности со специальными программами, выполняющими (самостоятельно или в связке с другими похожими средствами) функции защиты, такие как аутентификацию и идентификацию каждого пользователя, разграничение доступа, запись всех событий в системе, шифрование данных и т.п. в соответствии с ГОСТ Э 51241-2008. Для предотвращения нелегального доступа посторонних лиц к данным и информации нужно обеспечить надежные механизмы распознавания каждого пользователя (или отдельных групп). Для этого могут применяться различные приспособления: ключи, магнитные карты, дискеты и т.д.

*Перспективные методы защиты информации* основаны на том, что с увеличением интеграции узлов и компонентов в устройстве обработки информации усложняется проведение специальной проверки данного устройства на наличие в нем модулей, выполняющих несанкционированные, с точки зрения пользователя, действия. При размещении на кристалле нескольких миллионов транзисторов ничто не мешает несколько тысяч из них выделить для выполнения каких-либо специальных действий. И никто в перспективе не сможет дать вам гарантию, что этот узел, к примеру, не уничтожит всю информацию на компьютере по команде свыше. А миниатюризация мобильных средств хранения информации упрощает их хищение. Кроме того, с ростом сложности системы понижается ее надежность. Увеличение производительности вычислительной системы и емкости каналов связи позволяет злоумышленникам в более короткие сроки произвести расшифровку паролей и ключей доступа, организовать более интенсивное воздействие на узел инфор-

мационной сети, и похитить большие объемы информации, а использование открытых каналов передачи информации облегчает возможность перехвата трафика.

Ситуация в области защиты информации сегодня складывается для «защитников» не лучшим образом. В сфере информационных технологий средства защиты всегда отставали от средств нападения (возможно, умышленно) как минимум на один шаг. При современных скоростях прогресса и существующих подходах отставание будет только увеличиваться. Выход из этого кризиса возможен только при кардинальном изменении подходов к организации защиты информации. Система информационной безопасности должна быть одним из компонентов, составляющих основу системы обработки информации.

Одной из основных проблем при решении данного вопроса является отставание России в информационно-технологической сфере, особенно в производстве.

Второй серьезной проблемой является современная методология организации защиты информации. Технологически процесс выглядит так: на входе имеется типовой компьютер, т.е. законченная интегрированная система, и на него устанавливается еще один чужеродный элемент – система защиты информации. Недостаток данного подхода в том, что в этом случае из двух отдельных системообразующих компонентов не получается единой защищенной системы, которая, согласно теории системного анализа, должна приобрести новые свойства, отсутствующие у исходных компонентов. В данном случае есть компьютер и средство защиты. Убирая средство защиты, компьютер продолжает нормально функционировать. В случае переноса средства защиты на другой компьютер получается новая «защищенная система». Такой подход фундаментально не правильный. При удалении одного из базовых компонентов система должна перестать существовать. Вирус попадает в антивирусную базу только после того, как произойдет определенное количество его запусков в системе. До сих пор не существует нормальной математической модели «жизнедеятельности» этих «существ», на которую можно было бы опереться разработчикам. Средства защиты нового поколения должны иметь возможность идентифицировать любой вирус по признакам его деятельности, независимо от того, старый он или новый.

Из всего вышесказанного следует, что таков минимальный перечень требований к узлам сети, предназначенной для обработки защищаемой информации. При реализации комплексов обработки информации с учетом вышеприведенных требований, или аналогичных им, возможно создание полноценной системы защиты. С учетом современных вычислительных и коммуникационных мощностей, применение функций системы защиты не должно оказывать заметных тормозящих действий на процессы обработки информации, стоимость таких комплексов, естественно, будет выше обычных, что затрагивает также и финансовую сторону вопроса.

## Литература

1. *Адаменко М.А.* Основы классической криптологии. Секреты шифров и кодов. М.: ДМК Пресс, 2012. 256 с.
2. *Бирюков А.А.* Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.
3. *Гашков С.Б., Применко Э.А., Черепнев М.А.* Криптографические методы защиты информации. М.: Академия, 2010. 304 с.

4. *Гладышев А.И., Аборкина Е.С.* Вопросы применения существующих методов оценки сложности информационных систем // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ, управление». 2016. Вып. 1–2. С. 114–118.
5. ГОСТ Р 51275-2006. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2007. 7 с.
6. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № Пр-646. М., 2016. 16 с.
7. *Платонов В.* Программно-аппаратные средства защиты информации: учебник. М.: Academia, 2014. 336 с.
8. *Родичев Ю.А.* Нормативная база и стандарты в области информационной безопасности: учеб. пособие. СПб.: Питер, 2017. 256 с.
9. *Семененко В.А.* Информационная безопасность: учеб. пособие. 4-е изд., стер. М.: МГИУ, 2010. 277 с.

## Literatura

1. *Adamenko M.A.* Osnovy klassicheskoy kriptologii. Sekrety shifrov i kodov. M.: DMK Press, 2012. 256 s.
2. *Biryukov A.A.* Informatsionnaya bezopasnost': zashchita i napadenie. M.: DMK Press, 2012. 474 s.
3. *Gashkov S.B., Primenko E.A., Cherepnev M.A.* Kriptograficheskie metody zashity informatsii. M.: Akademia, 2010. 304 s.
4. *Gladyshev A.I., Aborkina E.S.* Voprosy primeneniya sushchestvuyushchikh metodov otsenki slozhnosti informatsionnykh sistem // Vestnik Rossiyskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz, upravlenie". 2016. Vyp. 1–2. S. 114–118.
5. GOST R 51275-2006. Ob"ekt informatizatsii. Faktory, vozdeystvuyushchie na informatsiyu. Obshchie polozheniya. M., 2007. 7 s.
6. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii ot 5 dekabrya 2016 g. № Pr-646. M., 2016. 16 s.
7. *Platonov V.* Programmno-apparatnye sredstva zashity informatsii: uchebnik. M.: Academia, 2014. 336 s.
8. *Rodichev Yu.A.* Normativnaya baza i standarty v oblasti informatsionnoy bezopasnosti: ucheb. posobie. SPb.: Piter, 2017. 256 s.
9. *Semenenko V.A.* Informatsionnaya bezopasnost': ucheb. posobie. 4-e izd., ster. M.: MGIU, 2010. 277 s.

DOI: 10.25586/RNU.V9187.19.02.P.123 УДК 681.518:339.13

С.В. Хаджиева

# ПРИМЕНЕНИЕ МЕТОДА ЖАДНОГО АЛГОРИТМА ДЛЯ ФОРМИРОВАНИЯ КОМАНД В IT-КОМПАНИИ В УСЛОВИЯХ AGILE-ТРАНСФОРМАЦИИ

Рассматривается возможность применения эвристического метода жадного алгоритма для решения класса прикладных задач, ориентированных на формирование IT-команд по функциональным ролям из имеющегося состава сотрудников в условиях Agile-трансформации.

*Ключевые слова:* IT-команда, IT-компания, Agile-трансформация, формирование команд, функциональная роль, жадный алгоритм, эвристический алгоритм, оптимизационная задача, задача о разбиении множества.