УДК 004.056

Д.С. Милько, А.В. Данеев

Множество вариантов решений для задачи выбора мер защиты объектов критической информационной инфраструктуры

Для защиты значимых объектов критической информационной инфраструктуры (КИИ) необходимо разрабатывать системы защиты информации, которые включают организационные и технические меры. Сложность при разработке систем защиты информации представляет не только выбор мер защиты информации, который зависит от множества критериев, но и составление множества всех вариантов, подходящих для решения указанной задачи, если объект критической информационной инфраструктуры является государственной (муниципальной) информационной системой или информационной системой персональных данных. В настоящей работе проведен сравнительный анализ всех возможных организационных и технических мер защиты объектов информатизации для получения сводного множества вариантов мер защиты информации.

Ключевые слова: поддержка принятия решений, критическая информационная инфраструктура, меры защиты информации, информационные системы персональных данных, государственные информационные системы.
DOI: 10.21293/1818-0442-2023-26-1-82-90

Защита объектов критической информационной инфраструктуры (КИИ) является ключевой задачей, решение которой необходимо для достижения устойчивого функционирования Российской Федерации при проведении в отношении нее компьютерных атак. Необходимость проработки данного направления подтверждается значительным ростом заинтересованности вопросами обеспечения безопасности КИИ как со стороны исследователей [1, 2], так со стороны предприятий [3, 4] и государственных структур. Проблемы защищенности критической информационной инфраструктуры исследуются по всему миру, в частности в США [5, 6], Великобритании [7, 8].

В соответствии с законодательством РФ реализация мероприятий по защите КИИ начинается с установления требований к обеспечению безопасности на основании обследования и категорирования объектов КИИ на предприятиях (рис. 1). Далее на основании полученных результатов экспертным путем производится выбор конкретных мер защиты, необходимых и достаточных для защиты каждого объекта КИИ [9]. Выбранные меры защиты должны быть внедрены в виде системы защиты объекта КИИ, которая включает средства защиты информации (СЗИ). После внедрения и проведения соответствующих испытаний система защиты объекта КИИ принимается в постоянную эксплуатацию. В ходе эксплуатации указанная система защиты может быть модернизирована, а также по решению предприятия выведена из эксплуатации вместе с объектом КИИ.

На схеме, изображенной на рис. 1, наглядно продемонстрированы точки принятия решений о выборе мер защиты информации (ЗИ) в ходе жизненного цикла системы защиты информации для объекта КИИ.

Некорректно принятые решения по выбору мер ЗИ в каждой из указанных точек способны негативно повлиять на защищенность объектов КИИ. Таким образом, результаты выбора мер ЗИ непосредственно влияют на защищенность КИИ Российской Федерации в целом и каждого из объектов КИИ в частности.

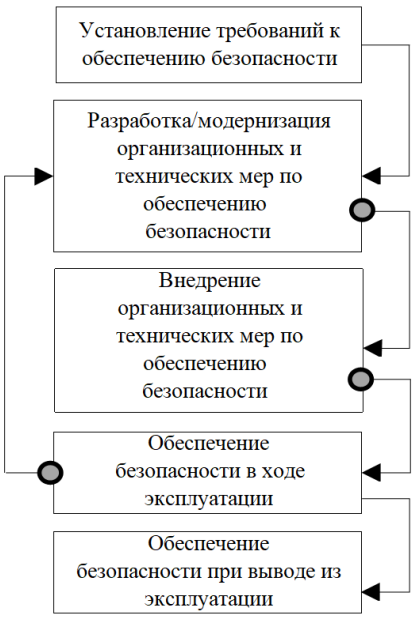

Рис. 1. Стадии (этапы) жизненного цикла системы защиты информации значимого объекта КИИ

В настоящий момент в соответствии с Доктриной информационной безопасности [10] состояние информационной безопасности России характеризуется недостаточным кадровым обеспечением. Проблема нехватки квалифицированных кадров в области информационной безопасности остается не решенной в течение длительного времени, что также подтверждается в научных работах А.В. Царегородцева, Е.П. Цацкиной (2019), В.Н. Азарова, Ю.И. Гудкова (2015), А.А. Малюка (2011) [11–13].

С учетом кадрового дефицита для решения сложной и ответственной задачи выбора мер ЗИ объекта КИИ зачастую невозможно принять оптимальное решение учитывая только субъективное мнение специалистов. По этой причине необходимо привлечение специальных информационно-аналити-

ческих технологий, опирающихся на математические методы [14].

С учетом указанной проблематики была поставлена задача разработки программного обеспечения (ПО), позволяющего автоматически поддерживать принятие решений по выбору мер защиты объектов КИИ. С технической точки зрения решение данной задачи сводится к выбору совокупности наилучших вариантов для достижения намеченной цели – выбора мер ЗИ.

Применение математических методов предполагает построение математической модели объекта анализа. Ситуация принятия решения в таком случае должна быть описана в формальном виде с указанием доступных вариантов действий и возможных последствий их реализации [14].

В рамках данной работы было проведено составление полного списка мер ЗИ, которые могут быть рассмотрены в качестве множества вариантов V (от нем. variant) решения поставленной задачи.

Указанное множество вариантов V должно соответствовать следующим критериям:

– не содержать дублирований;

– быть универсальным для всех объектов информатизации вне зависимости от их видов;

– подходить для объектов КИИ всех категорий значимости (в том числе не значимых).

Подход к составлению множества вариантов решений

Множество вариантов решений V в первом приближении должно включать меры по обеспечению безопасности объектов КИИ, перечисленные в приложении к требованиям [9]. Однако с практической точки зрения данный набор мер является только так называемым «базовым» набором мер.

По причине отсутствия отдельного методического документа с информацией о мерах защиты объектов КИИ на практике методом аналогии используется методический документ для государственных информационных систем [15].

В соответствии с определением термина «объект информатизации» из ГОСТ 51275–2006 [16] объекты КИИ относятся к объектам информатизации. Существующие виды объектов информатизации перечислены в нормативном документе [17]:

– государственные информационные системы (ГИС), в том числе региональные и муниципальные;

– информационные системы управления производством, используемые организациями оборонно-промышленного комплекса (ИС ОПК);

– помещения, предназначенные для ведения конфиденциальных переговоров (защищаемые помещения);

– значимые объекты КИИ;

– информационные системы персональных данных (ИСПДн);

– автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (АСУ КВО).

Защищаемые помещения могут быть исключены из рассмотрения, так как они не могут являться объектами КИИ в соответствии с нормативной базой [18]. Также в данной работе не будут рассмотрены меры защиты ИС ОПК, так как нормативные документы, касающиеся указанного вида объекта информатизации, являются документами ограниченного доступа.

С учетом того, что объекты КИИ относятся к объектам информатизации, выбор мер защиты для объектов КИИ должен состоять из 4 этапов (рис. 2):

а) определение базового набора мер ЗИ для установленного уровня значимости объекта КИИ;

б) адаптация базового набора мер ЗИ применительно к структурно-функциональным характеристикам объекта КИИ, информационным технологиям, особенностям функционирования объекта КИИ;

в) уточнение адаптированного базового набора мер ЗИ с учетом не выбранных ранее мер ЗИ для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

г) дополнение уточненного адаптированного базового набора мер ЗИ мерами, обеспечивающими выполнение требований о ЗИ, установленными иными нормативными правовыми актами в области ЗИ (требования о ЗИ в ГИС, ИСПДн, АСУ КВО).

В соответствии с указанным порядком для значимого объекта КИИ необходимо реализовать дополненный уточненный адаптированный базовый набор мер ЗИ, а не только базовый набор мер, представленный в приложении к требованиям [9]. Следовательно, необходимо добавить меры ЗИ из других нормативных документов, которые не представлены в приложении к требованиям [9].

Для выполнения критерия универсальности для всех объектов информатизации множество вариантов решений V должно включать максимально возможное количество мер защиты, перечисленных в требованиях о ЗИ (для объектов КИИ, ГИС, ИСПДн, АСУ КВО) и иных нормативных правовых актах, распространяющих свое действие на объекты КИИ. Данный тезис может быть представлен на языке множеств путем объединения (1).

$$V = V_1 \cup V_2 \cup V_3, \quad (1)$$

где V_1 – подмножество вариантов решений, включающее базовый набор мер для объектов КИИ (приложение к требованиям [9]) и АСУ КВО (приложение № 2 к требованиям [19], совпадает с приложением к тебованиям [9]); V_2 – подмножество вариантов решений, включающее базовый набор мер для ГИС (приложение № 2 к требованиям [20]); V_3 – подмножество вариантов решений, включающее базовый набор мер для ИСПДн (приложение к составу и содержанию мер [21]).

Документ [15] также содержит усиления для каждой из указанных мер, которые в некоторых условиях могут быть рассмотрены как дополнитель-

ное подмножество вариантов. Однако рассмотрение указанных усилений мер защиты в рамках поставленной задачи показало, что все они входят в состав мер, уже содержащихся в [20], хотя и более строго описывают способы их реализации с учетом усиления. По этой причине усиления мер ЗИ из документа [15] были исключены из рассмотрения в данной работе.

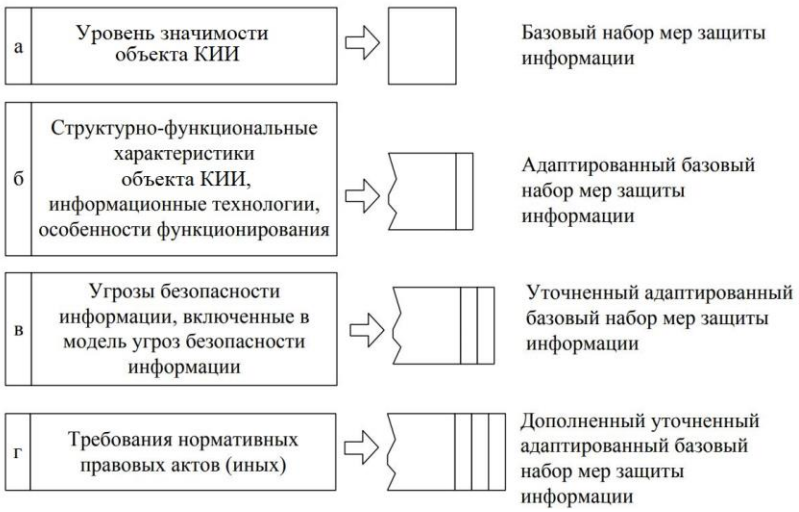

Рис. 2. Общий порядок действий при выборе мер защиты информации объекта КИИ для их реализации

Суть данной работы заключается в составлении подмножества всех возможных вариантов решений V. Элементы подмножеств вариантов решений V_1, V_2, V_3 во многом совпадают между собой. Однако часть элементов из разных подмножеств незначительно отличаются друг от друга в формулировках. По этой причине объединение подмножеств вариантов решений V_1, V_2, V_3 может быть осуществлено только после их аналитического сравнения.

Результаты составления множества вариантов решений

Результаты аналитического сравнения подмножеств вариантов решений V_1, V_2, V_3 и полученный сводный перечень мер защиты объектов КИИ (множество V) представлены в таблице.

Результаты составления множества вариантов решений

№ п/п	Описание сущности меры ЗИ	Обозначение меры в нормативном документе ФСТЭК России, разработанном для защиты		
		КИИ (V_1)	ГИС (V_2)	ИСПДн (V_3)
I. Идентификация и аутентификация (ИАФ)				
1	*2*	*3*	*4*	*5*
1	Регламентация правил ИАФ путем составления соответствующего документа	ИАФ.0	–	–
2	Определение всех внутренних пользователей, их действий и подтверждение их подлинности	ИАФ.1	ИАФ.1	ИАФ.1
3	Определение и подтверждение подлинности всех технических средств (ТС)	ИАФ.2	ИАФ.2	ИАФ.2
4	Контроль и актуализация идентификаторов	ИАФ.3	ИАФ.3	ИАФ.3
5	Контроль средств подтверждения подлинности пользователей	ИАФ.4	ИАФ.4	ИАФ.4
6	Определение всех внешних пользователей, их действий и подтверждение их подлинности	ИАФ.5	ИАФ.6	ИАФ.6
7	Обоюдное подтверждение подлинности	ИАФ.6	–	–
8	ЗИ при подтверждении подлинности с использованием каналов связи	ИАФ.7	–	–
9	Визуальное скрытие пароля при его вводе	–	ИАФ.5	ИАФ.5
10	Определение и подтверждение подлинности всех объектов доступа	–	ИАФ.7	–
II. Управление доступом (УПД)				
11	Регламентация правил УПД путем составления соответствующего документа	УПД.0	–	–
12	Контроль и актуализация всех учетных записей	УПД.1	УПД.1	УПД.1
13	Настройка прав для всех учетных записей в соответствии с матрицей доступа	УПД.2	УПД.2	УПД.2
14	Блокирование несанкционированной загрузки сторонней операционной системы (ОС)	УПД.3	УПД.17	УПД.17
15	Выделение учетных записей для администрирования	УПД.4	УПД.4	УПД.4
16	Настройка учетных записей для администрирования	УПД.5	УПД.5	УПД.5
17	Блокирование учетной записи при многократном вводе неверного пароля	УПД.6	УПД.6	УПД.6
18	Информирование пользователя о соблюдении мер ЗИ при каждом входе в рабочую сессию	УПД.7	УПД.7	УПД.7
19	Информирование пользователя о его предыдущей рабочей сессии	УПД.8	УПД.8	УПД.8
20	Ограничение для пользователя количества одновременных рабочих сессий	УПД.9	УПД.9	УПД.9

Продолжение таблицы

1	*2*	*3*	*4*	*5*
21	Возможность блокирования рабочей сессии по решению пользователя (или по таймеру в случае его отсутствия на рабочем месте)	УПД.10	УПД.10	УПД.10
22	Настройка прав для всех учетных записей, которые могут выполняться до процедуры ИАФ	УПД.11	УПД.11	УПД.11
23	Контроль определяющих признаков объектов доступа в соответствии с матрицей доступа	УПД.12	УПД.12	УПД.12
24	Использование VPN для удаленной работы	УПД.13	УПД.13	УПД.13
25	Контроль и ограничение действий пользователей, подключаемых из сторонних систем	УПД.14	УПД.16	УПД.16
26	Ограничение использования беспроводных ТС	–	УПД.14	УПД.14
27	Ограничение использования мобильных ТС	–	УПД.15	УПД.15
III. Ограничение программной среды (ОПС)				
28	Регламентация правил ОПС путем составления соответствующего документа	ОПС.0	–	–
29	Контроль и ограничение действий компонентов ПО	ОПС.1	ОПС.1	ОПС.1
30	Контроль и ограничение установки ПО	ОПС.2	ОПС.2	ОПС.2
31	Контроль и ограничение действий с временными файлами	ОПС.3	ОПС.4	ОПС.4
IV. Защита машинных носителей информации (ЗНИ)				
32	Регламентация правил ЗНИ путем составления соответствующего документа	ЗНИ.0	–	–
33	Регистрация и учет всех накопителей информации	ЗНИ.1	ЗНИ.1	ЗНИ.1
34	Контроль и ограничение доступа к накопителям информации	ЗНИ.2	ЗНИ.2	ЗНИ.2
35	Контроль и ограничение выноса накопителей информации за границу контролируемой зоны (КЗ)	ЗНИ.3	ЗНИ.3	ЗНИ.3
36	Исключение возможности несанкционированного доступа к информации на накопителях, в том числе в случае их выноса за границу КЗ	ЗНИ.4	ЗНИ.4	ЗНИ.4
37	Контроль и ограничение интерфейсов подключения накопителей информации	ЗНИ.5	ЗНИ.5	ЗНИ.5
38	Контроль и ограничение обмена информацией с накопителями	ЗНИ.6	ЗНИ.6	ЗНИ.6
39	Контроль подключения накопителей информации	ЗНИ.7	ЗНИ.7	ЗНИ.7
40	Обеспечение возможности затирания информации на накопителях в случае необходимости	ЗНИ.8	ЗНИ.8	ЗНИ.8
V. Аудит безопасности (АУД) / Регистрация событий безопасности (РСБ) / Контроль (анализ) защищенности информации (АНЗ)				
41	Регламентация правил АУД, РСБ и АНЗ путем составления соответствующего документа	АУД.0	РСБ.1, РСБ.2	РСБ.1, РСБ.2
42	Регистрация и учет состава ТС, ПО и СЗИ	АУД.1	АНЗ.4	АНЗ.4
43	Периодический анализ и нейтрализация возможности эксплуатации уязвимостей	АУД.2	АНЗ.1	АНЗ.1
44	Обеспечение надежности информации о времени и дате	АУД.3	РСБ.6	РСБ.6
45	Автоматическое ведение журналов безопасности	АУД.4	РСБ.3	РСБ.3
46	Контроль и анализ всех сетевых пакетов	АУД.5	–	–
47	Защита журналов безопасности	АУД.6	РСБ.7	РСБ.7
48	Периодический просмотр журналов безопасности и при необходимости принятие мер	АУД.7	РСБ.5	РСБ.5
49	Реагирование на ошибки ведения журналов безопасности	АУД.8	РСБ.4	РСБ.4
50	Регистрация в журналах безопасности действий всех пользователей	АУД.9	РСБ.8	–
51	Периодическая самопроверка	АУД.10	–	–
52	Периодическая проверка с привлечением независимых экспертов	АУД.11	–	–
53	Периодическая проверка корректности настроек ПО	–	АНЗ.3	АНЗ.3
54	Периодическая проверка корректности реализации мер ИАФ и УПД	–	АНЗ.5	АНЗ.5
VI. Антивирусная защита (АВЗ)				
55	Регламентация правил АВЗ путем составления соответствующего документа	АВЗ.0	–	–
56	Внедрение средств антивирусной защиты (САВЗ)	АВЗ.1	АВЗ.1	АВЗ.1
57	Применение специализированных САВЗ для отдельных служб (e-mail, web и т.п.)	АВЗ.2	–	–
58	Применение специализированных САВЗ для проверки отдельных типов файлов (запакованные файлы, файлы запуска ПО и файлы, защищенные криптографическими алгоритмами)	АВЗ.3	–	–
59	Обновление вирусных баз САВЗ	АВЗ.4	АВЗ.2	АВЗ.2
60	Применение САВЗ разных разработчиков	АВЗ.5	–	–
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
61	Регламентация правил СОВ путем составления соответствующего документа	СОВ.0	–	–
62	Внедрение СОВ	СОВ.1	СОВ.1	СОВ.1
63	Обновление баз правил СОВ	СОВ.2	СОВ.2	СОВ.2
VIII. Обеспечение целостности (ОЦЛ)				
64	Регламентация правил ОЦЛ путем составления соответствующего документа	ОЦЛ.0	–	–
65	Периодическая проверка целостности ПО	ОЦЛ.1	ОЦЛ.1	ОЦЛ.1
66	Периодическая проверка целостности защищаемых данных	ОЦЛ.2	ОЦЛ.2	ОЦЛ.2
67	Контроль и ограничение действий пользователей при вводе информации	ОЦЛ.3	ОЦЛ.6	ОЦЛ.6
68	Контроль и ограничение информации, которая может быть введена пользователем	ОЦЛ.4	ОЦЛ.7	ОЦЛ.7
69	Применение принципа «foolproof» при вводе информации	ОЦЛ.5	ОЦЛ.8	ОЦЛ.8
70	Исключение возможности привязки информации к физическому лицу	ОЦЛ.6	–	–
71	Ограничение вывода защищаемых данных во внешние системы	–	ОЦЛ.5	ОЦЛ.5

Продолжение таблицы

1	2	3	4	5
IX. Обеспечение доступности (ОДТ) / Обеспечение целостности (ОЦЛ)				
72	Регламентация правил ОДТ и ОЦЛ путем составления соответствующего документа	ОДТ.0	–	–
73	Дублирование ТС с целью работоспособности в случае отказа отдельных компонентов	ОДТ.1	ОДТ.1	ОДТ.1
74	Дублирование средств обеспечения	ОДТ.2	ОДТ.2	ОДТ.2
75	Реагирование на отказы отдельных компонентов	ОДТ.3	ОДТ.3	ОДТ.3
76	Дублирование информации на резервных накопителях	ОДТ.4	ОДТ.4	ОДТ.4
77	Восстановление информации с резервных накопителей в аварийной ситуации	ОДТ.5	ОДТ.5	ОДТ.5
78	Восстановление ПО с резервных накопителей в аварийной ситуации	ОДТ.6	ОЦЛ.3	ОЦЛ.3
79	Создание кластеров ТС и ПО с целью работоспособности в случае отказа отдельных компонентов	ОДТ.7	ОДТ.6	–
80	Периодическая проверка качества предоставления услуг сторонней информационной инфраструктуры	ОДТ.8	ОДТ.7	–
X. Защита среды виртуализации (ЗСВ)				
81	Регламентация правил ЗСВ путем составления соответствующего документа	–	–	–
82	Реализация ИАФ в виртуальной инфраструктуре (ВИ)	–	ЗСВ.1	ЗСВ.1
83	Контроль и ограничение доступа в ВИ в соответствии с матрицей доступа	–	ЗСВ.2	ЗСВ.2
84	Автоматическое ведение журналов безопасности ВИ	–	ЗСВ.3	ЗСВ.3
85	Контроль и ограничение информационных потоков ВИ	–	ЗСВ.4	ЗСВ.4
86	Блокирование несанкционированной загрузки ВИ	–	ЗСВ.5	ЗСВ.5
87	Контроль и ограничение действий с виртуальными машинами и защищаемой информацией	ЗИС.39	ЗСВ.6	ЗСВ.6
88	Периодическая проверка целостности ВИ и настроек ВИ	–	ЗСВ.7	ЗСВ.7
89	Дублирование частей ВИ с целью работоспособности в случае отказа отдельных компонентов	ДНС.4	ЗСВ.8	ЗСВ.8
90	Внедрение и контроль САВЗ в ВИ	–	ЗСВ.9	ЗСВ.9
91	Дробление ВИ в соответствии с матрицей доступа	–	ЗСВ.10	ЗСВ.10
XI. Защита технических средств и систем (ЗТС)				
92	Регламентация правил ЗТС путем составления соответствующего документа	ЗТС.0	–	–
93	Защита от перехвата информативных сигналов по техническим каналам утечки информации	ЗТС.1	ЗТС.1	ЗТС.1
94	Определение КЗ	ЗТС.2	ЗТС.2	ЗТС.2
95	Ограничение доступа в КЗ	ЗТС.3	ЗТС.3	ЗТС.3
96	Ограничение несанкционированного просмотра данных с мониторов, индикаторов и т.п.	ЗТС.4	ЗТС.4	ЗТС.4
97	Блокирование техногенных угроз (неблагоприятных погодных условий, сбоев систем водоснабжения, водоотведения, охлаждения, электропитания и т.п.)	ЗТС.5	ЗТС.5	ЗТС.5
98	Обозначение ТС метками в соответствии с уровнями защищенности данных, подлежащих обработке	ЗТС.6	–	–
XII. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) / Обеспечение целостности (ОЦЛ) / Управление доступом (УПД)				
99	Регламентация правил ЗИС, ОЦЛ и УПД путем составления соответствующего документа	ЗИС.0	–	–
100	Определение пользователей, администраторов и их полномочий	ЗИС.1	ЗИС.1	ЗИС.1
101	Определение и защита границ при обмене информацией со сторонними системами	ЗИС.2	ЗИС.23	–
102	Реализация многоуровневой защиты	ЗИС.3	–	–
103	Дробление на сегменты и обеспечение безопасности каждого из сегментов	ЗИС.4	ЗИС.17	ЗИС.17
104	Определение всех частей, в которых могут не применяться СЗИ	ЗИС.5	–	–
105	Контроль и ограничение информационных потоков	ЗИС.6	УПД.3	УПД.3
106	Выделение изолированной части инфраструктуры («песочницы») для безопасного тестирования ПО	ЗИС.7	–	–
107	Обфускация применяемых информационных технологий	ЗИС.8	ЗИС.28	–
108	Применение ОС и ПО разных разработчиков	ЗИС.9	ЗИС.25	–
109	Применение ПО, способного работать в ОС разных типов	ЗИС.10	ЗИС.26	–
110	Приоритезация процессов	ЗИС.11	ЗИС.2	ЗИС.2
111	Выделение изолированной части памяти для работы ПО	ЗИС.12	ЗИС.19	ЗИС.19
112	Обеспечение неизменности резервных копий, файлов конфигураций и прочих файлов, которые не должны быть изменены в процессе эксплуатации	ЗИС.13	ЗИС.15	ЗИС.15
113	Применение для работы с ПО накопителей информации, предназначенных только для чтения	ЗИС.14	ЗИС.18	ЗИС.18
114	Ограничение количества узлов, имеющих возможность обмена e-mail со сторонними системами	ЗИС.15	–	–
115	Блокирование массовых рассылок	ЗИС.16	ОЦЛ.4	ОЦЛ.4
116	Предотвращение утечек защищаемых данных	ЗИС.17	–	–
117	Контроль и ограничение доступа к некоторым web-ресурсам	ЗИС.18	–	–
118	Шифрование данных при отправке по общедоступным каналам связи	ЗИС.19	ЗИС.3	ЗИС.3
119	Защита канала связи администратора с СЗИ и пользователя с СЗИ	ЗИС.20	ЗИС.4	ЗИС.4
120	Предотвращение несанкционированного удаленного включения периферийного оборудования (аудио, видео и т.п.) без ведома пользователя	ЗИС.21	ЗИС.5	ЗИС.5

Продолжение таблицы

1	*2*	*3*	*4*	*5*
121	Синхронизация определяющих признаков объектов доступа при взаимодействии со сторонними системами	ЗИС.22	ЗИС.6	ЗИС.6
122	Контроль и ограничение применения мобильного кода	ЗИС.23	ЗИС.7	ЗИС.7
123	Контроль и ограничение передачи аудиоинформации (в т.ч. и речевой)	ЗИС.24	ЗИС.8	ЗИС.8
124	Контроль и ограничение передачи видеоинформации	ЗИС.25	ЗИС.9	ЗИС.9
125	Контроль правильности сопоставления сетевых (IP) адресов и сетевых имен (DNS)	ЗИС.26	ЗИС.10	ЗИС.10
126	Контроль неизменности сетевых соединений	ЗИС.27	ЗИС.11	ЗИС.11
127	Обеспечение неотвратимости факта отправки данных	ЗИС.28	ЗИС.12	ЗИС.12
128	Обеспечение неотвратимости факта принятия данных	ЗИС.29	ЗИС.13	ЗИС.13
129	Применение технологии «тонкий клиент»	ЗИС.30	ЗИС.14	ЗИС.14
130	Исключение пересылки данных методами, не предназначенными для этого	ЗИС.31	ЗИС.16	ЗИС.16
131	Обеспечение безопасности для беспроводных способов связи	ЗИС.32	ЗИС.20	ЗИС.20
132	Предотвращение возможности несанкционированного доступа пользователя к данным предыдущих пользователей	ЗИС.33	ЗИС.21	–
133	Предотвращение отказов в обслуживании (DoS, DDoS)	ЗИС.34	ЗИС.22	–
134	Прерывание сетевых соединений по таймеру бездействия	ЗИС.35	ЗИС.24	–
135	Использование ресурсов-приманок («honeypot») для выявления злоумышленника	ЗИС.36	ЗИС.27	–
136	Создание более защищенной конфигурации на случай возникновения нештатных ситуаций	ЗИС.37	ЗИС.29	–
137	Обеспечение безопасности мобильных ТС	ЗИС.38	ЗИС.30	–
	XIII. Реагирование на компьютерные инциденты (ИНЦ)			
138	Регламентация правил ИНЦ путем составления соответствующего документа	ИНЦ.0	–	–
139	Выявление событий безопасности и инцидентов безопасности	ИНЦ.1	–	ИНЦ.2
140	Доведение информации о событиях безопасности и инцидентах безопасности до ответственных лиц	ИНЦ.2	–	ИНЦ.3
141	Анализ событий безопасности и инцидентов безопасности	ИНЦ.3	–	ИНЦ.4
142	Устранение или минимизация последствий инцидентов	ИНЦ.4	–	ИНЦ.5
143	Реализация мероприятий по недопущению повторения инцидентов	ИНЦ.5	–	ИНЦ.6
144	Регистрация и защита данных о произошедших инцидентах	ИНЦ.6	–	–
145	Назначение ответственных лиц за ИНЦ	–	–	ИНЦ.1
	XIV. Управление конфигурацией (УКФ) / Ограничение программной среды (ОПС)			
146	Регламентация правил УКФ и ОПС путем составления соответствующего документа	УКФ.0	–	–
147	Определение объектов, связанных с конфигурацией	УКФ.1	–	–
148	Контроль изменений в конфигурации	УКФ.2	–	УКФ.2
149	Ограничение и контроль ПО, которое может быть установлено	УКФ.3	ОПС.3	ОПС.3
150	Автоматическое ведение журналов изменений	УКФ.4	–	–
151	Назначение ответственных лиц за УКФ	–	–	УКФ.1
152	Прогнозирование последствий изменений в конфигурации, а также согласование изменений с ответственным лицом	–	–	УКФ.3
153	Внесение информации об изменениях в документацию	–	–	УКФ.4
	XV. Управление обновлениями ПО (ОПО) / Контроль (анализ) защищенности информации (АНЗ)			
154	Регламентация правил ОПО и АНЗ путем составления соответствующего документа	ОПО.0	–	–
155	Загрузка новой версии ПО от доверенного информационного ресурса	ОПО.1	–	–
156	Сверка даты выпуска, размера и контрольных сумм новой версии ПО	ОПО.2	–	–
157	Тестирование новой версии ПО	ОПО.3	–	–
158	Контроль установки новой версии ПО	ОПО.4	АНЗ.2	АНЗ.2
	XVI. Планирование мероприятий по обеспечению безопасности (ПЛН)			
159	Регламентация правил ПЛН путем составления соответствующего документа	ПЛН.0	–	–
160	Ведение планов мероприятий, касающихся информационной безопасности	ПЛН.1	–	–
161	Контроль соблюдения планов мероприятий, касающихся информационной безопасности	ПЛН.2	–	–
	XVII. Обеспечение действий в нештатных ситуациях (ДНС)			
162	Регламентация правил ДНС путем составления соответствующего документа	ДНС.0	–	–
163	Создание плана ДНС	ДНС.1	–	–
164	Обучение работников и отработка ДНС	ДНС.2	–	–
165	Дублирование мест размещения в случае возникновения нештатных ситуаций	ДНС.3	–	–
166	Реализация возможности восстановления в случае возникновения нештатных ситуаций	ДНС.5	–	–
167	Реализация мероприятий по недопущению повторения нештатных ситуаций	ДНС.6	–	–
	XVIII. Информирование и обучение персонала (ИПО)			
168	Регламентация правил ИПО путем составления соответствующего документа	ИПО.0	–	–
169	ИПО об актуальных угрозах и способах противодействия им	ИПО.1	–	–
170	ИПО правилам безопасной эксплуатации	ИПО.2	–	–
171	Организация практических занятий ИПО по правилам безопасной эксплуатации	ИПО.3	–	–
172	Проверка уровня знаний работников об актуальных угрозах и о правилах безопасной эксплуатации	ИПО.4	–	–

Выводы по результатам сравнительного анализа

Подмножество вариантов V_1 включает в свой состав наибольшее количество мер ЗИ. В первую очередь это меры, касающиеся разработки политик информационной безопасности (меры подмножества V_1 с обозначениями ИАФ.0, УПД.0, ОПС.0, ЗНИ.0, АУД.0, АВЗ.0, СОВ.0, ОЦЛ.0, ОДТ.0, ЗТС.0, ЗИС.0, ИНЦ.0, УКФ.0, ОПО.0, ПЛН.0, ДНС.0, ИПО.0). По причине отсутствия мер ЗСВ в подмножестве V_1 мера ЗСВ.0 была также добавлена в сводный перечень, так как процедура защиты ЗСВ также должна быть регламентирована.

Кроме этого, подмножество вариантов V_1 в отличие от подмножеств V_1 и V_3 содержит уникальные меры ЗИ:

– аудит безопасности (меры подмножества V_1 с обозначениями АУД.1, АУД.5, АУД.10, АУД.11);

– антивирусная защита (меры подмножества V_1 с обозначениями АВЗ.2, АВЗ.3, АВЗ.5);

– обеспечение целостности (мера подмножества V_1 с обозначением ОЦЛ.6);

– обеспечение доступности (мера подмножества V_1 с обозначением ОДТ.6);

– защита ТС и систем (мера подмножества V_1 с обозначением ЗТС.6);

– защита информационной (автоматизированной) системы и ее компонентов (меры подмножества V_1 с обозначениями ЗИС.3, ЗИС.5, ЗИС.7, ЗИС.14, ЗИС.15, ЗИС.17, ЗИС.18, ЗИС.39);

– управление конфигурацией (меры подмножества V_1 с обозначениями УКФ.1, УКФ.4);

– управление обновлениями ПО (меры подмножества V_1 с обозначениями ОПО.1, …, ОПО.4);

– планирование мероприятий по обеспечению безопасности (меры подмножества V_1 с обозначениями ПЛН.1, ПЛН.2);

– обеспечение действий в нештатных ситуациях (меры подмножества V_1 с обозначениями ДНС.1, …, ДНС.6);

– информирование и обучение персонала (меры подмножества V_1 с обозначениями ИПО.1, …, ИПО.4).

С другой стороны, подмножество V_1 не включает в себя меры по ЗИ из подмножества V_2:

– идентификация и аутентификация (меры подмножества V_2 с обозначениями ИАФ.5, ИАФ.7);

– управление доступом (меры подмножества V_2 с обозначениями УПД.14, УПД.15);

– контроль (анализ) защищенности информации (меры подмножества V_2 с обозначениями АНЗ.2, …, АНЗ.5);

– обеспечение целостности (мера подмножества V_2 с обозначением ОЦЛ.5);

– защита среды виртуализации (меры подмножества V_2 с обозначениями ЗСВ.1, …, ЗСВ.10);

– защита информационной (автоматизированной) системы и ее компонентов (мера подмножества V_2 с обозначением ЗИС.18).

В дополнение к указанным выше мерам подмножество V_3 включает следующие уникальные меры ЗИ:

– реагирование на компьютерные инциденты (мера подмножества V_3 с обозначением ИНЦ.1);

– управление конфигурацией (меры подмножества V_3 с обозначениями УКФ.1, УКФ.3, УКФ.4).

По результатам сравнительного анализа также стоит обратить внимание на то, что несколько мер ЗИ из подмножества V_1 совпадают с мерами из подмножеств V_2 и V_3, находясь при этом в различных группах мер. Так, например, мера АУД.3 из подмножества V_1 соответствует мере РСБ.6 подмножеств V_2 и V_3 (п. 44, таблица). Аналогичным образом мера ЗИС.16 из подмножества V_1 соответствует мере ОЦЛ.4 подмножеств V_2 и V_3 (п. 112, таблица).

Заключение

Разработан полный сводный перечень вариантов мер ЗИ. Данный перечень не содержит дублирований, является универсальным и может применяться как для объектов КИИ (значимых и не значимых), так и для ГИС, ИСПДн, АСУ КВО всех классов и уровней защищенности.

Сравнительный анализ показал, что различные перечни мер ЗИ являются однородными, но имеют различия. Перечень мер защиты объектов КИИ является самым объемным и аналогичен перечню мер защиты АСУ КВО. Перечни мер защиты ГИС и ИСПДн во многом идентичны друг другу и имеют ряд уникальных мер ЗИ, не встречающихся в перечне мер защиты объектов КИИ.

Также в результате анализа были максимально раскрыты названия всех мер ЗИ, которые встречаются в различных перечнях мер. Это позволяет однозначно трактовать каждую из мер ЗИ, встречающихся в различных источниках.

Результаты анализа использованы для разработки ПО поддержки принятия решений при выборе мер защиты объектов КИИ в качестве множества из 172 вариантов решения поставленной задачи $V = \{v^1, v^2, \ldots, v^{172}\}$.

Полученные результаты могут применяться исследователями защищенности объектов КИИ, предприятиями при разработке, внедрении и модернизации мер защиты объектов КИИ, а также регуляторами в сфере ЗИ в рамках контроля защищенности объектов КИИ.

За помощь в проведении сравнительного анализа выражается благодарность Репину Дмитрию Андреевичу, студенту группы 729-1 направления подготовки «Информационная безопасность автоматизированных систем» ТУСУРа.

Литература

1. Гаськова Д.А. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры / Д.А. Гаськова, А.Г. Массель // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 42–48.

2. Голдобина А.С. Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры / А.С. Голдобина, Ю.А. Исаева, В.В. Селифанов, А.М. Климова, П.С. Зенкин // Доклады ТУСУР. – 2018. – Т. 21, № 4. – С. 51–58.

3. Нормативные документы в области ГосСОПКА и безопасности КИИ [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/knowledgebase/terminology-gossopka-kii-full-version/, свободный (дата обращения: 04.12.2022).

4. Защита критической информационной инфраструктуры (конспект лекции) [Электронный ресурс]. – Режим доступа: https://www.securityvision.ru/blog/zashchita-kriticheskoy-informatsionnoy-infrastruktury-konspekt-lektsii/, свободный (дата обращения: 04.12.2022).

5. Katzan H. Contemporary issues in cybersecurity // Journal of Cybersecurity Research (JCR). – 2016. – Vol. 1, No. 1. – PP. 1–6. DOI: 10.19030/jcr.v1i1.9745.

6. Dadashzadeh M. Choosing IT platforms in the Age of Stuxnet // Journal of Cybersecurity Research (JCR). – 2017. – Vol. 2, no. 1. – PP. 17–26. DOI: 10.19030/jcr.v2i1.10076.

7. Securing industrial control system environments: The missing piece / U.D. Ani , N. Daniel, F. Oladipo, S.E. Adewumi // Journal of Cyber Security Technology. – 2018. – Vol. 2, No. 3-4. – P. 131–163. DOI: 10.1080/23742917.2018.1554985.

8. Ani U.P.D. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective / U.P.D. Ani, H. He, A. Tiwari // Journal of Cyber Security Technology. – 2017. – Vol. 1, No. 1. – PP. 32–74. DOI: 10.1080/23742917.2016.1252211.

9. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239, свободный (дата обращения: 04.12.2022).

10. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201612060002, свободный (дата обращения: 04.12.2022).

11. Царегородцев А.В. Влияние информационного общества на подготовку обучающихся в сфере информационной безопасности / А.В. Царегородцев, Е.П. Цацкина // Вестник Моск. гос. лингвистич. ун-та. Образование и педагогич. науки. – 2019. – № 4 (833). – С. 191–199.

12. Азаров В.Н. Некоторые проблемы инженерной подготовки в области информационных технологий и пути их решения / В.Н. Азаров, Ю.И. Гудков // Вестник ИрГТУ (Иркутск). – 2015. – № 3 (98). – С. 233–237.

13. Малюк А.А. Кадровое обеспечение информационной безопасности // Государственная служба (Москва). – 2011. – № 5. – С.75–79.

14. Подиновский В.В. Идеи и методы теории важности критериев в многокритериальных задачах принятия решений. – М.: Наука, 2019. – 103 с.

15. Методический документ Меры защиты информации в государственных информационных системах Утвержден ФСТЭК России 11 февраля 2014 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument, свободный (дата обращения: 04.12.2022).

16. ГОСТ Р 51275–2006. Защита информации Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Режим доступа: https://www.altell.ru/legislation/standards/51275-2006.pdf, свободный (дата обращения: 04.12.2022).

17. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/2270-prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77, свободный (дата обращения: 04.12.2022).

18. Федеральный закон от 26.07.2017 № 187-ФЗ. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201707260023, свободный (дата обращения: 04.12.2022).

19. Приказ ФСТЭК России от 14 марта 2014 г. № 31 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31, свободный (дата обращения: 04.12.2022).

20. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17, свободный (дата обращения 04.12.2022).

21. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21, свободный (дата обращения: 04.12.2022).

Милько Дмитрий Сергеевич
Аспирант каф. информационнных систем и защиты информации (ИСиЗИ) Иркутского государственного ун-та путей сообщения (ИрГУПС)
Чернышевского ул., 15, г. Иркутск, Россия, 664074
Тел.: +7 (395-2) 638-359
ORCID: 0000-0002-6259-6749
Эл. почта: dmitry.s.milko@gmail.com

Данеев Алексей Васильевич
Д-р техн. наук, проф. каф. ИСиЗИ ИрГУПС
Чернышевского ул., 15, г. Иркутск, Россия, 664074
ORCID: 0000-0003-4288-824X
Тел.: +7 (395-2) 63-83-59
Эл. почта: daneev@mail.ru

Milko D.S., Daneev A.V.

Multiple of solutions for the choosing measures task to cybersecurity of critical infrastructure

Cybersecurity of critical information infrastructure is achieved by developing an information security system. It includes organizational and technical measures. The complexity in its development is not only the choice of information security measures (it depends on many criteria), but also the compilation of a set of all options suitable for solving this problem, especially if the object of critical information infrastructure is a state (municipal) information system or a personal data information system. In this paper, a comparative analysis of all possible protection measures is carried out to obtain a consolidated set of options.

Keywords: decision support, critical infrastructure, information security measures, personal data information systems, government information systems.
DOI: 10.21293/1818-0442-2023-26-1-82-90

References

1. Gaskova D.A., Massel A.G. [The technology of cyber threat analysis and risk assessment of cybersecurity violation of critical infrastructure] *Cybersecurity Issues*, 2019, no. 2(30), pp. 42–48 (in Russ.).

2. Goldobina A.S., Isaeva Yu.A., Selifanov V.V., Klimova A.M., Zenkin P.S. [Building an adaptive three-tier model of management processes for the information security system of critical information infrastructure objects] *Proceedings of TUSUR University*, 2018. Vol. 21, no. 4, pp. 51–58 (in Russ.).

3. [Regulatory documents in the field of public procurement and critical infrastructure security] (In Russ.). Available at: https://www.ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version/, free (Accessed: December 4, 2022).

4. [Protection of critical information infrastructure (lecture summary)]. Available at: https://www.securityvision.ru/blog/zashchita-kriticheskoy-informatsionnoy-infrastruktury-konspekt-lektsii/, free (Accessed: December 4, 2022) (in Russ.).

5. Katzan H. Contemporary issues in cybersecurity. *Journal of Cybersecurity Research (JCR)*, 2016. Vol. 1, no. 1, pp. 1–6. DOI: 10.19030/jcr.v1i1.9745.

6. Dadashzadeh M. Choosing IT platforms in the Age of Stuxnet. *Journal of Cybersecurity Research (JCR)*, 2017, vol. 2, no. 1, pp. 17–26. DOI 10.19030/jcr.v2i1.10076.

7. Ani U.D., Daniel N., Oladipo F., Adewumi S.E. Securing industrial control system environments: The missing piece. *Journal of Cyber Security Technology*, 2018. vol. 2, no. 3–4, pp. 131–163. DOI: 10.1080/23742917.2018.1554985.

8. Ani U.P.D., He H., Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, 2017, vol. 1, no. 1, pp. 32–74. DOI: 10.1080/23742917.2016.1252211.

9. Order of the FSTEC of Russia dated December 25, 2017, no. 239. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239, free (Accessed: December 4, 2022).

10. Information Security Doctrine of the Russian Federation Available at: http://publication.pravo.gov.ru/Document/View/0001201612060002, free (Accessed: December 4, 2022).

11. Tsaregorodcev A.V., Tsatskina E.P. [The impact of the information society on the training of information security students]. *Bulletin of the Moscow State Linguistic University. Education and Pedagogical Sciences*, 2019, no. 4 (833), pp. 191–199 (in Russ.).

12. Azarov A.N., Gudkov Yu.I. [Some problems of engineering training in the field of information technology and ways to solve them]. *Bulletin of ISTU (Irkutsk)*, 2015, no. 3 (98), pp. 233–237 (in Russ.).

13. Malyuk A.A. [Information security staffing]. *Public Service (Moscow)*, 2011, no. 5, pp. 75–79 (in Russ.).

14. Podinovsky V.V. [Ideas and methods of the theory of the importance of criteria in multi-criteria decision-making tasks]. Moscow, Science, 2019. 103 p. (in Russ.).

15. Methodical document Information security measures in State information systems Approved by the FSTEC of Russia on February 11, 2014. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument, free (Accessed: December 4, 2022). (in Russ.).

16. [GOST R 51275-206. Information security. The object of informatization. Factors affecting information. General terms]. Available at: https://www.altell.ru/legislation/standards/51275-2006.pdf, free (Accessed: December 4, 2022) (in Russ.).

17. Order of the FSTEC of Russia dated April 29, 2021 No. 77. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/2270-prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77, free (Accessed: December 4, 2022).

18. Federal Law of 26.07.2017 No. 187. Available at: http://publication.pravo.gov.ru/Document/View/0001201707260023, free (Accessed: December 4, 2022) (in Russ.).

19. Order of the FSTEC of Russia dated March 14, 2014 No. 31. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31, free (Accessed: December 4, 2022).

20. Order of the FSTEC of Russia dated February 11, 2013 No. 17. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17, free (Accessed: December 4, 2022).

21. Order of the FSTEC of Russia dated February 18, 2013 No. 21. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21, free (Accessed: December 4, 2022).

Dmitry S. Milko
Graduate student, Department of Information Systems and Information Security, Irkutsk State Transport University
15, Chernyshevsky st., Irkutsk, Russia, 664074
ORCID: 0000-0002-6259-6749
Phone: +7 (395-2) 63-83-59
Email: dmitry.s.milko@gmail.com

Alexey V. Daneev
Doctor of Science in Engineering, Professor,
Department of Information Systems and Information Security, Irkutsk State Transport University
15, Chernyshevsky st., Irkutsk, Russia, 664074
ORCID: 0000-0003-4288-824X
Phone: +7 (395-2) 63-83-59
Email: daneev@mail.ru