УДК 004.056 + 658.1:622 + 681.518 Вестник УрФО № 3(25) / 2017, с. 24–33

Захаров А. А., Римша А. С., Харченко А. М., Зулькарнеев И. Р.

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ ПРОЦЕССАМИ ГАЗОДОБЫВАЮЩЕГО ПРЕДПРИЯТИЯ

В настоящее время на предприятиях газодобывающей отрасли используют автоматизированные системы, позволяющие повысить эффективность и контроль технологического процесса. Эти предприятии являются частью критической информационной инфраструктуры России, опасным производственным объектом, при эксплуатации которого могут возникнуть аварийные ситуации, причиной которых может быть, в том числе, и недостаточная защищенность автоматизированных систем управления технологическими процессами.

Для анализа защиты типовой иерархической структуры предприятия по добыче газа предложена математическая модель его информационной инфраструктуры. Рассматривается принцип работы каждого уровня такой системы, идентифицируются активы и определяется технология моделирования средств защиты информации. Приводится перечень основных уязвимостей системы. Формулируются этапы оценки уязвимости, на основе которых выделяются основные угрозы. После идентификации рисков проводится оценка их величины. Рассматриваются этапы внедрения средств защиты и их влияние на сокращение возможного ущерба.

Ключевые слова: *газодобывающая организация, критическая информационная инфраструктура, информационная безопасность, математическая модель, оценка рисков.*

Zakharov A. A., A.S. Rimsha, A.M. Kharchenko, I.R. Zulkarneev

ANALYSIS OF INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS FOR TECHNICAL PROCESSES OF A GAS PRODUCING ENTERPRISE

At present, the enterprises of the gas industry are using automated systems to a greater or lesser extent, which make it possible to increase the efficiency and control the technological process. The principle of operation of automation systems of technological processes at a gas producing enterprise is in many respects like the solutions used in other industrial enterprises, but they also have their own peculiarities. They represent a dangerous production facility, during the operation of which there can be emergencies, caused, including by the incorrect operation of automated systems.

This paper is devoted to the construction of a mathematical model for analysis of the protection of a typical hierarchical structure of the automated process control system for gas production. The principle of operation of each level of such a system is considered, the assets of the whole system are identified. The technology of modeling IIS is determined. The list of the main vulnerabilities of the system is given. The stages of vulnerability assessment are formulated based on which the main threats to the process control system are highlighted. After identifying the risks, a risk analysis is performed, the result of which is the overall estimated risk value. The stages of implementation of IIS measures, as well as their impact on possible damage, are considered.

Keywords: gas producing organization, critical information infrastructure, information security, mathematical model, risk assessment.

Введение

Для автоматизации технологических процессов в газодобывающей отрасли используются автоматизированные системы управления технологическим процессом (АСУ ТП), построенные на базе промышленных логических контроллеров (ПЛК) [1].

Одной из задач корректного функционирования АСУ ТП является обеспечение информационной безопасности (ИБ) этих систем. Проблемы защиты АСУ ТП от вредоносного программного обеспечения (ПО) Stuxnet, Duqu, Flame и другие обсуждаются в работах [2-4].

Важно подчеркнуть бытовавшее представление о том, что функционирование АСУ ТП сложно нарушить благодаря следующим обстоятельствам:

– ПО каждой АСУ ТП, как правило, проприетарное и закрытое;

– в локальной сети пользователей на верхнем уровне АСУ ТП проблемы с безопасностью можно решить организацией корректной политики ограничения доступа;

– проникновение в АСУ ТП связано с большими интеллектуальными затратами, а выгода для злоумышленника не очевидна.

Однако недавние инциденты с заражением компьютеров предприятий, занимающихся добычей нефти и газа, в «Роснефть», «Башнефть» [5] вирусами типа WannaCry [6] или Petya, использующими уязвимость устаревшего протокола SMBv1, свидетельствуют об обратном. Более того, тот факт, что предприятия передают данные по Ethernet во внешние сети (например, в центральный офис), показывают, что такие системы необходимо защищать, в том числе, и по причине возможного использования информационных технологий как инструмента давления и противобор-

ства. Это нашло свое отражение в Доктрине информационной безопасности Российской Федерации 2016 года и Стратегии национальной безопасности США 2015 года.

Отметим, что, даже отделив физически технологическую сеть АСУ ТП от сетей общего пользования, нельзя исключать возможность заражения вирусом, случайно принесенным пользователем на внешнем носителе. Все это заставляет по-новому поставить вопросы, связанные с информационной безопасностью предприятий, использующих АСУ ТП.

В соответствии с последними изменениями законодательства о ключевой информационной инфраструктуре (КИИ) от 26 июля 2017 г., принятыми федеральными законами 183-ФЗ, 193-ФЗ и 194-ФЗ, АСУ ТП относятся к КИИ и подлежат обязательной категоризации и защите [7] в соответствии с требованиями нормативно-правовых актов, обязательному контролю со стороны соответствующих ФОИВ. Также вводится уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, содержащейся в КИИ [8].

Предварительный анализ типовых информационных системы АСУ ТП газодобывающего предприятия, протоколов передачи информации и информационных ресурсов показывает сложность их взаимодействий и, как следствие, потенциальную возможность реализации тех или иных угроз ИБ [9, 10].

Поскольку статистику по инцидентам, связанным с нарушением ИБ, трудно собрать в должном объеме, то актуальной задачей представляется моделирование системы защиты ИС АСУ ТП типового газодобывающего предприятия, с целью оценки рисков информационной безопасности, оптимизации расходов на ИБ и конкретизации рекомендаций к организационным и технологическим мероприятиям, повышающим защищенность ИС АСУ ТП [11].

Существуют различные подходы к моделированию систем защиты информации (СЗИ), отражающие те или иные аспекты систем защиты [9, 12 - 15]:

– обобщенные модели систем защиты;

– модели, использующие подходы теории вероятности и нейронных сетей;

– модели, построенные с использованием теории сетей Петри–Маркова;

– модели, основанные на теории конечных автоматов;

– модели, построенные с использованием теории графов;

– модели, использующие теорию нечетких множеств;

– модели, построенные с использованием энтропийного подхода.

Модели, использующие теорию вероятности и нейронные сети, идеально работают, например, при анализе аномалий сетевого трафика из внешней сети, когда можно на основе статистики классифицировать аномалию и принять решение о блокировке определенного трафика.

Модели на основе сетей Петри–Маркова, как и модели, использующие автоматы Мура, хорошо себя зарекомендовали для анализа управления вероятностью успешной реализации НСД по времени (с использованием статических данных) [16,17].

Модели ИБ, использующие теорию графов, хорошо работают в системах поддержки принятия решений с использованием экспертов, когда, например, необходимо оценить безопасность того или иного пути реализации процесса, а для оптимизации выбора наиболее безопасного маршрута используется модифицированный алгоритм Дейкстры [18].

Модели на основе нечетких множеств (модель Мамдани, TSK- модели и др.) можно использовать для оценки рисков ИБ с помощью хорошо спланированных экспериментов и экспертов, способных грамотно оценить результат работы модели, т.е. полученный риск, по входным данным. Обычно хорошо работают для конкретных информационных процессов в защищаемой ИС [19].

Модели ИБ, построенные на основе энтропийного подхода, используются для выявления возможности идентификации пользователей веб-ресурсов [20].

Как правило, подход к моделированию выбирают, ориентируясь на параметры, используемые в качестве входной информации, и те результаты расчетов, которые получены на выходе. Обычно входная информация базируется на имеющейся статистике для существующих ИС и/или данных экспертов. Модели могут использоваться на этапе проектирования ИС, но чаще их используют на этапах эксплуатации и сопровождения, проведения мониторинга и аудита систем защиты информации.

Предлагаемая методология

Для выбора конкретной технологии мо-

делирования защиты ИС АСУ ТП формализуем бизнес-процессы типового газодобывающего предприятия, которое представляет собой территориально распределенную структуру, начинающуюся от кустов газовых скважин и заканчивающуюся центральным диспетчерским пунктом.

Управление технологическим процессом требует применения специальных технологических решений построения сетей передачи данных. Упрощенная структура АСУ ТП типового предприятия газодобывающей отрасли строится по иерархическому принципу. Обычно в промышленных АСУ ТП выделяют три уровня [1, 21]:

– *нижний уровень, или уровень ввода данных, исполнительных устройств* — датчики (датчики температуры, давления, расхода, и т.д.) и исполнительных механизмов (регулирующая и запорная арматура);

– *средний уровень, или уровень автоматического управления* — промышленные контроллеры, управляющие исполнительными механизмами и, при необходимости, передающие данные с датчиков на верхний уровень;

– *верхний уровень, или уровень операторского управления* — централизованное дистанционное управление, основанное на SCADA (supervisory control and data acquisition) и современных разработках в области информационных технологий (сервера ввода/вывода, коммутационное оборудование, рабочие места операторов и диспетчеров, базы данных, ПО для сбора данных, визуализации и мониторинга хода технологического процесса).

Введем основные обозначения:

$c^{sensor} = \{c_1^{sensor}, \dots, c_{a_1}^{sensor}\}$ - множество всех датчиков, используемых в технологическом процессе;

$c^{mechanism} = \{c_1^{mechanism}, \dots, c_{a_2}^{mechanism}\}$ - множество исполнительных механизмов;

$c^{PLC} = \{c_1^{PLC}, \dots, c_{a_3}^{PLC}\}$ - множество всех ПЛК;

$c^{server} = \{c_1^{server}, \dots, c_{a_4}^{server}\}$ - множество серверов ввода/вывода;

$c^{network} = \{c_1^{network}, \dots, c_{a_5}^{network}\}$ - множество элементов сетевого оборудования;

$c^{workstation} = \{c_1^{workstation}, \dots, c_{a_6}^{workstation}\}$ - множество автоматизированных рабочих мест (АРМ).

Тогда все многообразие компонентов, используемых в АСУ ТП газодобывающего предприятия, можно представить в виде множества $C = \{c^{sensor}, c^{mechanism}, c^{PLC}, c^{server}, c^{network}, c^{workstation}\}$. (1)

На физическом уровне для передачи данных между компонентами используется четыре типа сетей связи:

– электрические линии — $electrical$;

– волоконно-оптические линии — $fiber$;

– беспроводная связь — $wireless$;

– многопарные медные линии — UTP.

Таким образом, множество типов связи между компонентами c_i и c_j для передачи данных можно представить:

$$s_{ij} = \{electrical, fiber, wireless, UTP\}. \quad (2)$$

Множество типов связи между всеми компонентами образует многомерный массив, размерность которого определяется числом компонентов системы и представляет собой матрицу типов связи:

$$S = \begin{vmatrix} 0 & \cdots & s_{1j} & \cdots & s_{1i} & \cdots & s_{1n} \\ \cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{j1} & \cdots & 0 & \cdots & s_{ji} & \cdots & s_{jn} \\ \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots \\ s_{i1} & \cdots & s_{ij} & \cdots & 0 & \cdots & s_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \cdots \\ s_{n1} & \cdots & s_{nj} & \cdots & s_{ni} & \cdots & 0 \end{vmatrix}. \quad (3)$$

На логическом уровне в зависимости от производителя и типа оборудования используются промышленные протоколы (семейство протоколов Modbus, промышленная сеть PROFIBUS и т.д.). Между рабочими станциями и сетевым оборудованием, используется Ethernet. Сигналы, передающиеся по электрическим линиям, можно разделить на аналоговые, дискретные и цифровые. Обозначим множество способов передачи данных между компонентами c_i и c_j

$$pr_{ij} = \{pr_1, \dots, pr_b\}. \quad (4)$$

По аналогии с (3) множество способов передачи данных между всеми компонентами представим в виде матрицы:

$$Pr = \begin{vmatrix} 0 & \cdots & pr_{1j} & \cdots & pr_{1i} & \cdots & pr_{1n} \\ \cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots \\ pr_{j1} & \cdots & 0 & \cdots & pr_{ji} & \cdots & pr_{jn} \\ \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots \\ pr_{i1} & \cdots & pr_{ij} & \cdots & 0 & \cdots & pr_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \cdots \\ pr_{n1} & \cdots & pr_{nj} & \cdots & pr_{ni} & \cdots & 0 \end{vmatrix}. \quad (5)$$

Исходя из этого, связь между компонентами c_i и c_j будет иметь вид упорядоченной пары: тип связи и способ передачи данных – (s_{ij}, pr_{ij}).

Таким образом, ПЛК c_i^{PLC}, получив по од-

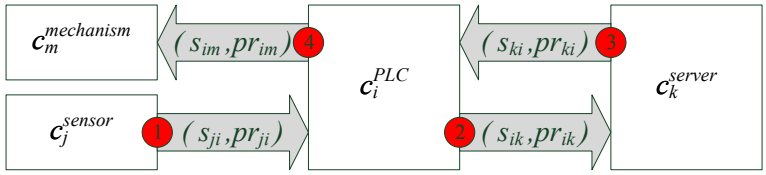

Рис. 1. Схема взаимодействия компонентов

ному из типов связи s_{ji} и соответствующим способом передачи данных pr_{ji} информацию от датчика c_j^{sensor}, отправляет информацию на верхний уровень c_k^{server} через (s_{ik}, pr_{ik}) и в зависимости от встроенных алгоритмов или указаний от *SCADA*-системы через (s_{ki}, pr_{ki}), отправляет по (s_{im}, pr_{im}) команду на выполнение определенных операций исполнительному механизму $c_m^{mechanism}$ (рис. 1).

Всем существенным с точки зрения защиты технологического процесса активам соответствует некая ценность, зависящая от степени его влияния на прибыль организации и уровнем ущерба (в финансовом, репутационном, социальном, промышленном и других планах), который может понести организация при выводе из строя, компрометации или некорректном функционировании данного актива. Объединим ценность активов во множество

$$A = \{A_1, \dots, A_o\}. \quad (6)$$

Согласно (1), (3) и (5) мощность такого множества будет равна $\boldsymbol{o = |C| + |S| + |Pr|}$.

Для выбора конкретной технологии моделирования защиты АСУ ТП в первую очередь будем использовать формализованную структуру компонентов и связей АСУ ТП (1-6) и такие критерии как:

– простота определения входных параметров модели (модель может использовать различные данные в качестве исходных, однако возможности получения этих данных могут быть задачами различной сложности);

– уровень подготовки и оснащенности злоумышленника;

– вероятность реализации той или иной угрозы, риски, связанные с этой угрозой и возможность рассчитать вероятный ущерб в результате реализации угрозы;

– возможность учесть разнородность компонентов системы каждого уровня (1-3) и связь между ними.

– возможность учета требования по защите АСУ ТП в соответствии с действующим законодательством;

– возможность рассчитать время обнаружения атаки в зависимости от используемых средств защиты, уязвимостей в них и уровня подготовки и оснащенности злоумышленника;

– при атаках на функционирующую систему возможна ситуация, когда на определенном этапе с помощью технологий обнаружения вторжения и/или оперативных действий персонала по соответствующему регламенту атака будет заблокирована. Важно определить среднее время от начала атаки до ее блокировки.

Анализ приведенных критериев показывает, что на первом этапе можно воспользоваться обобщенной моделью АСУ ТП типового газодобывающего предприятия вида:

$$K = \{C, S, Pr, A, T, V, P, D, R, L\},$$

где ***C*** – множество компонентов системы;

S – множество типов связи между всеми компонентами;

Pr – множество способов передачи между компонентами;

A – множество стоимостей всех активов организации;

T – множество угроз;

$\boldsymbol{V_i}$ – множество уязвимостей угрозы ;

P – множество характеристик угроз в виде вероятностных показателей;

D – множество мероприятий по снижению риска;

R – множество оценочных величин риска;

L – множество требований законодательства по защите АСУ ТП.

Поскольку в газодобывающем предприятии конфиденциальность не является критическим объектом защиты [22], то далее под уязвимостью будем понимать проблемы безопасности, которые позволяют нарушить целостность и доступность информации в системе АСУ ТП. Множество уязвимостей обозначим $\boldsymbol{V = \{V_1, \dots, V_m\}}$.

Каждая уязвимость может по-разному влиять на отдельный актив [23]. Таким образом, влияние уязвимостей на активы можно представить в виде матрицы уязвимостей и их влияние на актив.

	V_1	V_2	...	V_m
A_1	v_{11}	v_{12}	...	v_{1m}
A_2	v_{21}	v_{21}	...	v_{2m}
...	...	...	...	
A_o	v_{o1}	v_{o2}	...	v_{om}

Влияние одной уязвимости на множество активов можно рассчитать по следующей формуле:

$$V_j = \sum_{i=1}^{o} v_{ij} \times A_i \qquad (7)$$

где v_{ij} – воздействие уязвимости V_j на актив A_i.

Обозначим через множество угроз, а множество характеристик угроз в виде вероятностных показателей через . Каждая угроза представляет собой совокупность уязвимостей, но каждая уязвимость может по-своему влиять на реализацию угрозы, поэтому введем коэффициент потенциального воздействия уязвимости на угрозу – *d*.

При реализации угрозы нарушается технологический процесс, результатом которого может быть выход из строя компонентов системы. Под ущербом, нанесенным в таком случае, будем понимать совокупность всех уязвимостей конкретной угрозы с учетом потенциального воздействия каждой [24]. Определим матрицу угроз, которая отражает взаимосвязь угроз с уязвимостями.

	V_1	V_2	…	V_m
T_1	t_{11}	t_{12}	…	t_{1m}
T_2	t_{21}	t_{21}	…	t_{2m}
…	…	…	…	
T_g	t_{g1}	t_{g2}	…	t_{gm}

Так как под ущербом мы подразумеваем реализацию угрозы, то оценка ущерба от конкретной угрозы будет определяться совокупностью уязвимостей, которые с ней связаны:

$$T_h = \sum_{j=1}^{m} t_{hj} \times V_j = \sum_{j=1}^{m} \left(t_{hj} \times \sum_{i=1}^{n} v_{ij} \times A_j \right) \qquad (8)$$

где t_{hj} – воздействие уязвимости V_j на угрозу T_h.

Определим риск, как возможность того, что произойдет неблагоприятное событие, имеющее последствие (ущерб) T_h с вероятностью наступления этого события p_h [25]. Далее будем подразумевать, что риск зависит от реализации угрозы T_h. Таким образом, общая оценка величины риска системы будет представлять сумму последствий реализации всех угроз:

$$R = \sum_{i=1}^{g} R_i = \sum_{i=1}^{g} p_i \times T_i \qquad (9)$$

Для полной оценки величины ущерба организации необходимо учитывать не только величину риска в зависимости от реализации угроз, но и возможный ущерб от игнорирования требований законодательства по защите АСУ ТП и КИИ. Так как данный ущерб оценивается не только количественно, но и качественно, а требования являются обязательными для выполнения организациями, эксплуатирующих КИИ, то дополнительно следует учитывать затраты на реализацию этих требований как сумму затрат на выполнение конкретного требования L_i:

$$L = \sum_{i=1}^{l} L_i \qquad (10)$$

При этом надо учитывать, что в случае, если величина ущерба R_i от реализации угрозы T_i будет меньше величины затраты L_i, то целесообразно использовать компенсирующую меру, которая позволит сделать стоимость затрат меньшей, чем величина ущерба. В случае отсутствия подобной компенсирующей меры необходимо обосновать неприменимость этого требования и исключить его из общего множества. После оценки затрат на реализацию требований и оптимизации затрат с использованием компенсирующих мер и исключением неприменимых делается новая оценка величины *L*.

Общую оценочную величину затрат на реализацию СЗИ обозначим как *C*. Под допустимым риском будем понимать риск, потери по которому не превышают определенной суммы прибыли, установленной в организации. Определим следующие условия:

1) минимальное значение *C* должно быть равно *L* для выполнения требований законодательства;

2) если $C < L + R$, то процесс внедрения мер СЗИ на этом шаге пропускается и осуществляется мониторинг системы;

2) если $C \geq L + R$, то необходимо разрабатывать программу мероприятий по снижению ущерба при реализации угроз;

Комплекс таких мероприятий, организационных и технических, называется мероприятиями СЗИ. Каждое мероприятие из СЗИ будет оказывать определенное влияние на совокупность угроз. С оставим матрицу СЗИ с учетом применения требований законодательства *L*.

	L_1	L_2	…	L_l
T_1	l_{11}	l_{12}	…	l_{1l}
T_2	l_{21}	l_{21}	…	l_{2l}
…	…	…	…	
T_g	l_{g1}	l_{g2}	…	l_{gl}

Исходя из матрицы СЗИ, можно рассчитать ущерб от угрозы T_h после внедрения l мероприятий СЗИ:

$$T_h^{'} = \sum_{i=1}^{l} l_{hi} \times T_h \qquad (11)$$

где l_{hi} – воздействие определенных законом мер L_i на угрозу T_h.

После внедрения СЗИ вероятность реализации угрозы T_h изменяется, принимая вид p'_h. Таким образом, после внедрения мер, определенных законодательством, меняется и оценочная величина риска R'_h. Далее необходимо провести разработку мероприятий по защите системы исходя из реализованных мер с учетом обновленных величин от реализации угроз T'_h. С учетом этих мероприятий итоговая матрица мер СЗИ будет выглядеть так:

	D_1	D_2	...	D_l
$T_1^{'}$	d_{11}	d_{12}	...	d_{1l}
$T_2^{'}$	d_{21}	d_{21}	...	d_{2l}
...	...	...	...	
$T_g^{'}$	d_{g1}	d_{g2}	...	d_{gl}

Исходя из матрицы СЗИ, можно рассчитать ущерб от угрозы T'_h после внедрения l мероприятий СЗИ:

$$T_h^{''} = \sum_{i=1}^{l} d_{hi} \times T_h^{'}$$

где d_{hi} – воздействие СЗИ на угрозу T'_h.

Соответственно меняется и оценочная величина риска R''_h.

Выводы

Перед внедрением мер важно рассчитать стоимость их реализации, исходя из выделенного бюджета ИБ и требований законодательства. Если стоимость мероприятий превышает допустимые расходы – необходимо скорректировать риски: отложить маловероятные на следующий цикл, а наиболее опасные риски понизить в рамках текущего бюджета.

Процесс управления рисками будет происходить до тех пор, пока значение общей оценочной величины риска R не опустится ниже допустимого уровня, установленного в организации, и стоимость внедрения таких мероприятий не превысит допустимые расходы.

Предложенная модель позволяет выполнить анализ и оценить риски информационной безопасности. Установив допустимый уровень общей оценочной величины риска, принимается решение о необходимости внедрения СЗИ. Процесс происходит до тех пор, пока оценочная величина риска не примет допустимый уровень.

Модель была использована для анализа рисков АСУ ТП газодобывающего предприятия, что позволило учесть влияние каждой уязвимости и на компоненты каждого уровня АСУ ТП и на связь между ними. Благодаря этой особенности были сделаны расчеты ущерба при некорректном функционировании всей системы в результате реализации даже одной угрозы.

Примечания

1. Сергеев Н. Е., Добровольский С. В. АСУ ТП цеха добычи нефти и газа // Известия ЮФУ. Технические науки. 2000. — №1. — С. 159

2. Shearer J., Symantec. W32.Stuxnet. URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

3. Symantec Corporation, Duqu: следующий Stuxnet. URL: http://www.symantec.com/ru/ru/outbreak/?id=stuxnet

4. Gostev À., Securelist, The Flame: Questions and Answers. URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

5. Кречетова А., Forbes Staff, Petya в «Роснефти»: нефтяная компания пожаловалась на мощную хакерскую атаку. URL: http://www.forbes.ru/kompanii/346997-rosneft-pozhalovalas-na-moshchnuyu-hakerskuyu-ataku

6. ProSoft, Разбудит ли вирус WannaCry промышленную Кибербезопасность. URL: https://tp.prosoft.ru/news/obzory-issledovaniya-analitika/175645/

7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

8. Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Рос-

сийской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

9. Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли // Доклады ТУСУР. 2013. — №2 (28). — С. 112-115

10. Крымский В. Г., Жалбеков И. М., Имильбаев Р. Р., Юнусов А. Р. Автоматизация управления технологическими процессами в газораспределительных сетях: проблемы, тенденции и перспективы // Электротехнические и информационные комплексы и системы. 2013. — №2. — С. 70-79

11. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. — №1 (9). — С. 73-79

12. Арьков П. А. Комплекс моделей для поиска оптимального проекта системы защиты информации // Известия ЮФУ. Технические науки. 2008. — №8. — С. 30-36

13. Данилова Е.А., Хохоля А.С., Золотарев В.В. Построение и анализ математических моделей эффективности и безопасности автоматизированных систем // Актуальные проблемы авиации и космонавтики. 2010. — №6. — С. 392-393

14. Варлатая С.К., Шаханова М.В. Математические модели динамики возникновения и реализации угроз информационной безопасности // Доклады ТУСУР. 2012. — №1-2 (25). — С. 7-11

15. Бондарь И.В. Методика построения модели угроз безопасности информации для автоматизированных систем // Вестник СибГУ им. М.Ф. Решетнева. 2012. — №3 (43). — С. 7-10

16. Миронова В. Г., Шелупанов А. А., Сопов М. А. Сети Петри-Маркова как инструмент создания аналитических моделей для основных видов несанкционированного доступа в информационной системе // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. — №. 1-2 (25). — С. 20-24

17. Меньших В.В., Петрова Е.В. Теоретическое обоснование и Синтез математической модели защищенной информационной системы ОВД как сети автоматов // Вестник ВИ МВД России. 2010. — №3. — С. 134-143

18. Ефимов Б. И. Применение алгоритмов теории графов для решения задач, связанных с обеспечением информационной безопасности в системах принятия решений //Системы управления и информационные технологии. 2009. Т. 35. — №. 1.3. — С. 342-346

19. Булдакова Т. И., Миков Д. А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2013. — №11. — С. 295-310

20. Захаров И.В., Забузов В.С., Фомин С.И., Фомин С.И., Эсаулов К.А. Способ априорной оценки возможности идентификации пользователей веб-ресурсов на основе энтропийного подхода // Современные проблемы науки и образования. 2014. — № 1. — С. 1-7

21. Чуркин Г. М., Великанов А. М., Тырин Е. А. К вопросу о выборе средств автоматизации АСУ ТП // Вестник СГТУ. 2013. — №1 (70). — С. 151-158

22. Духвалов А.П. Кибератаки на критически важные объекты вероятная причина катастроф // Вопросы кибербезопасности. 2014. — №3 (4). — С. 50-53

23. Дружинин Е., Карпов И., Гнедин Е., Бойко И., Симонова Ю. Безопасность АСУ ТП в цифрах // Москва: Positive Technologies, 2016. — С. 9

24. Пищик Б.Н. Безопасность АСУ ТП // ЖВТ. 2013. — №.5 — С. 170-175

25. Баранова Е.К., Мальцева А.Н. Анализ рисков информационной безопасности для малого и среднего бизнеса // Директор по безопасности. 2015. — №9 (69). — С. 58-63

References

1. Sergeev N. E., Dobrovolskii S. V. ASU TP tsekha dobychi nefti i gaza [APCS plant oil and gas] // Izvestiia IuFU. Tekhnicheskie nauki [Proceedings of the SFU. Technical science]. 2000. №1. P.159

2. Shearer J., Symantec. W32.Stuxnet. URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

3. Symantec Corporation, Duqu: sleduiushchii Stuxnet. URL: http://www.symantec.com/ru/ru/outbreak/?id=stuxnet

4. Gostev À., Securelist, The Flame: Questions and Answers. URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

5. Krechetova A., Forbes Staff, Petya v «Rosnefti»: neftianaia kompaniia pozhalovalas na moshchnuiu khakerskuiu ataku [Petya in Rosneft: the oil company complained of a powerful hacker attack]. URL: http://www.forbes.ru/kompanii/346997-rosneft-pozhalovalas-na-moshchnuyu-hakerskuyu-ataku

6. ProSoft, Razbudit li virus WannaCry promyshlennuiu Kiberbezopasnost [Will the WannaCry virus wake industrial Cybersecurity?]. URL: https://tp.prosoft.ru/news/obzory-issledovaniya-analitika/175645/

7. Federalnyi zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [On the Security of the Critical Information Infrastructure of the Russian Federation]

8. Federalnyi zakon ot 26.07.2017 № 194-FZ «O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i statiu 151 Ugolovno-protsessualnogo kodeksa Rossiiskoi Federatsii v sviazi s priniatiem Federalnogo zakona «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation in connection with the adoption of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation"]

9. Kirsanov S.V. Metod otsenki ugroz informatsionnoi bezopasnosti ASU TP gazovoi otrasli [The method of assessing threats to information security of the automated process control system of the gas industry] // Doklady TUSUR [TUSUR reports]. 2013. №2 (28). P.112-115

10. Krymskii V. G., Zhalbekov I. M., Imilbaev R. R., Iunusov A. R. Avtomatizatsiia upravleniia tekhnologicheskimi protsessami v gazoraspredelitelnykh setiakh: problemy, tendentsii i perspektivy [Automation of process control in gas distribution networks: problems, trends and prospects] // Elektrotekhnicheskie i informatsionnye kompleksy i sistemy [Electrical and information complexes and systems]. 2013. №2. P.70-79

11. Baranova E.K. Metodiki analiza i otsenki riskov informatsionnoi bezopasnosti [Methods of analysis and assessment of information security risks] // Obrazovatelnye resursy i tekhnologii [Educational resources and technologies]. 2015. №1 (9). P.73-79

12. Arkov P. A. Kompleks modelei dlia poiska optimalnogo proekta sistemy zashchity informatsii [A set of models for finding the optimal project of an information security system] // Izvestiia IuFU. Tekhnicheskie nauki [Proceedings of the SFU. Technical science]. 2008. №8. P.30-36

13. Danilova E.A., Khokholia A.S., Zolotarev V.V. Postroenie i analiz matematicheskikh modelei effektivnosti i bezopasnosti avtomatizirovannykh system [Construction and analysis of mathematical models of efficiency and safety of automated systems] // Aktualnye problemy aviatsii i kosmonavtiki [Actual problems of aviation and cosmonautics]. 2010. №6. P.392-393

14. Varlataia S.K., Shakhanova M.V. Matematicheskie modeli dinamiki vozniknoveniia i realizatsii ugroz informatsionnoi bezopasnosti [Mathematical models of the dynamics of the emergence and implementation of threats to information security] // Doklady TUSUR [TUSUR reports]. 2012. №1-2 (25). P.7-11

15. Bondar I.V. Metodika postroeniia modeli ugroz bezopasnosti informatsii dlia avtomatizirovannykh system [The method of constructing a model of information security threats for automated systems] // Vestnik SibGU im. M.F. Reshetneva [Bulletin of SibSU. M.F. Reshetnev]. 2012. №3 (43). P.7-10

16. Mironova V. G., Shelupanov A. A., Sopov M. A. Seti Petri-Markova kak instrument sozdaniia analiticheskikh modelei dlia osnovnykh vidov nesanktsionirovannogo dostupa v informatsionnoi sisteme [Petri-Markov networks as a tool for creating analytical models for the main types of unauthorized access in the information system] // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki [Reports of Tomsk State University of Control Systems and Radioelectronics]. 2012. №. 1-2 (25). P.20-24

17. Menshikh Valerii Vladimirovich, Petrova Elena Vladilenovna Teoreticheskoe obosnovanie i Sintez matematicheskoi modeli zashchishchennoi informatsionnoi sistemy OVD kak seti avtomatov [Theoretical justification and Synthesis of the mathematical model of the protected information system of ATS as a network of automats] // Vestnik VI MVD Rossii [Bulletin of the Ministry of Internal Affairs of Russia]. 2010. №3. P.134-143

18. Efimov B. I. Primenenie algoritmov teorii grafov dlia resheniia zadach, sviazannykh s obespecheniem informatsionnoi bezopasnosti v sistemakh priniatiia reshenii [Application of algorithms of graph theory for solving problems related to ensuring information security in decision-making systems] //Sistemy upravleniia i informatsionnye tekhnologii [Control Systems and Information Technology]. 2009. T. 35. №. 1.3. P. 342-346

19. Buldakova T. I., Mikov D. A. Otsenka informatsionnykh riskov v avtomatizirovannykh sistemakh s pomoshchiu neiro-nechetkoi modeli [Assessment of information risks in automated systems using a neural-fuzzy model] // Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana [Science and Education: a scientific edition of the MSTU. N.E. Bauman]. 2013. №11. P.295-310

20. Zakharov I.V., Zabuzov V.S., Fomin S.I., Fomin S.I., Esaulov K.A. Sposob apriornoi otsenki vozmozhnosti identifikatsii polzovatelei veb-resursov na osnove entropiinogo podkhoda [A method of a priori assessment of the possibility of identifying users of web resources based on the entropy approach] // Sovremennye problemy nauki i obrazovaniia [Modern problems of science and education]. 2014. № 1. P.1-7

21. Churkin G. M., Velikanov A. M., Tyrin E. A. K voprosu o vybore sredstv avtomatizatsii ASU TP [On the issue of choosing automation means for process control systems] // Vestnik SGTU [Bulletin of the CSTU]. 2013. №1 (70). P.151-158

22. Dukhvalov A.P. Kiberataki na kriticheski vazhnye obieekty veroiatnaia prichina katastrof [Cyberattacks on critical objects probable cause of accidents] // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. №3 (4). P.50-53

23. Druzhinin E., Karpov I., Gnedin E., Boiko I., Simonova Iu. Bezopasnost ASU TP v tsifrakh [Safety of automated control systems in figures] // Moskva: Positive Technologies, 2016. P.9

24. Pishchik B.N. Bezopasnost ASU TP [Safety of automated process control system] // ZhVT. 2013. №. P.170-175

25. Baranova E.K., Maltseva A.N. Analiz riskov informatsionnoi bezopasnosti dlia malogo i srednego biznesa [Analysis of information security risks for small and medium businesses] // Direktor po bezopasnosti [Director of Security]. 2015. №9 (69). P.58-63

ЗАХАРОВ Александр Анатольевич, доктор технических наук, профессор кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: azaharov@utmn.ru

РИМША Андрей Сергеевич, аспирант кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: RimshaAndrew@gmail.com

ХАРЧЕНКО Анастасия Михайловна, инженер ИТ отдела КИПиА и АСУ ТП АО «Ачимгаз». 629303, г. Новый Уренгой. мкр. Советский 7/2а. E-mail: Kharchenkoam.86@gmail.com

ЗУЛЬКАРНЕЕВ Искандер Рашитович, старший преподаватель кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: i.r.zulkarneev@utmn.ru

ZAKHAROV Alexander, Doctor of Technical Sciences, Professor of the Department of Information Security. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: azaharov@utmn.ru

RIMSHA Andrew, post-graduate student of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: RimshaAndrew@gmail.com

KHARCHENKO Anastasia, IT Engineer of the Instrumentation and Control Systems Department of Achimgaz JSC. Bld. 7/2a, Soviet Mdst., Noviy Urengoy, 629303. E-mail: Kharchenkoam.86@gmail.com

ZULKARNEYEV Iskander, senior lecturer of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: i.r.zulkarneev@utmn.ru