Математическая модель информационной безопасности АСУ ТП газового предприятия

А. С. Римша
Тюменский государственный университет
RimshaAndrew@gmail.com

А. Н. Югансон
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
a_yougunson@corp.ifmo.ru

***Аннотация*. В настоящее время на предприятиях газодобывающей отрасли используют автоматизированные системы, позволяющие повысить эффективность и контроль технологического процесса. Принцип работы систем автоматизации технологических процессов на газодобывающем предприятии во многом схож с решениями, используемыми на других промышленных предприятиях, но имеет, тем не менее, свои особенности. Предприятия по добыче газа представляют собой опасный производственный объект, 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 информационной безопасности. 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: математическая модель; информационная безопасность; газодобывающая организация; оценка рисков; киберфизическая система

I. Введение

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

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 информационной безопасности (ИБ) [2, 3].

Поскольку статистику по инцидентам, связанным с нарушением ИБ, трудно собрать в должном объеме, то актуальной задачей представляется моделирование системы ИБ 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 информационной системы (ИС) АСУ ТП [4].

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.

II. Предлагаемая методология

Для выбора конкретной технологии моделирования 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, 5]:

- *нижний уровень*, или *уровень ввода данных, исполнительных устройств* — датчики (датчики температуры, давления, расхода, и т.д.) и исполнительные механизмы (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, программное обеспечение для сбора данных, визуализации и мониторинга хода технологического процесса).

Введем основные обозначения:

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

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

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

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

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

$c^{workstation} = \{c_1^{workstation}, \ldots, c_{a_6}^{workstation}\}$ – множество автоматизированных рабочих мест.

Тогда множество всех типов оборудования, используемых в АСУ ТП газодобывающего предприятия, можно представить в следующем виде:

$$C = \{c^{sensor}, c^{mechanism}, c^{PLC}, c^{server}, c^{network}, c^{workstation}\} \quad (1)$$

В отличие от предложенной обобщённой математической модели АСУ ТП [6] для представления взаимодействия устройств друг с другом будет использоваться сетевая модель OSI, где каждому ее уровню (физическому, канальному, сетевому, транспортному, сеансовому, представления, прикладному) будет соответствовать матрица смежности, размерность которой определяется числом компонентов системы $|C|$, а в качестве значений будут указываться сетевые протоколы. Таким образом, множество взаимодействий устройств будет представлено в следующем виде:

$$S = \{S^1, \ldots, S^7\} \quad (2),$$

где $S^k = \begin{vmatrix} 0 & \ldots & s_{1j}^k & \ldots & s_{1i}^k & \ldots & s_{1n}^k \\ \ldots & 0 & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{j1}^k & \ldots & 0 & \ldots & s_{ji}^k & \ldots & s_{jn}^k \\ \ldots & \ldots & \ldots & 0 & \ldots & \ldots & \ldots \\ s_{i1}^k & \ldots & s_{ij}^k & \ldots & 0 & \ldots & s_{in}^k \\ \ldots & \ldots & \ldots & \ldots & \ldots & 0 & \ldots \\ s_{n1}^k & \ldots & s_{nj}^k & \ldots & s_{ni}^k & \ldots & 0 \end{vmatrix}$,

k – уровень модели OSI,

s_{ij} – протоколы взаимодействия.

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

$$A = \{A_1, \ldots, A_o\}. \quad (3)$$

Согласно (1) и (2) мощность такого множества будет равна $o = |C| + |S|$.

Поскольку в газодобывающем предприятии конфиденциальность не является критическим объектом защиты [7], то далее под уязвимостью будем понимать проблемы безопасности, которые позволяют нарушить целостность и доступность информации в системе АСУ ТП. Множество уязвимостей обозначим $V = \{V_1, \ldots, V_m\}$.

Каждая уязвимость может по-разному влиять на отдельный актив [8]. Таким образом, влияние уязвимостей на активы можно представить в виде матрицы уязвимостей и их влияние на актив.

ТАБЛИЦА I МАТРИЦА ВЛИЯНИЯ УЯЗВИМОСТЕЙ НА АКТИВЫ

	V_1	V_2	…	V_m
A_1	v_{11}	v_{12}	…	v_{1m}
A_2	v_{21}	v_{22}	…	v_{2m}
…	…	…	…	…
A_o	v_{o1}	v_{o2}	…	v_{om}

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

$$V_j = \sum_{i=1}^{o} v_{ij} \times A_i, \quad (4)$$

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

Обозначим через $T = \{T_1, \ldots, T_g\}$ множество угроз, а множество характеристик угроз в виде вероятностных показателей через $P = \{p_1, \ldots, p_g\}$, $h=1,2,\ldots,g$. 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 [9]. Определим матрицу угроз, которая отражает взаимосвязь угроз с уязвимостями.

ТАБЛИЦА II МАТРИЦА СВЯЗИ УГРОЗ И УЯЗВИМОСТЕЙ

	V_1	V_2	…	V_m
T_1	t_{11}	t_{12}	…	t_{1m}
T_2	t_{21}	t_{22}	…	t_{2m}
…	…	…	…	…
T_q	t_{q1}	t_{q2}	…	t_{qm}

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

$$T_h = \sum_{j=1}^{m} t_{hj} \times V_j = \sum_{j=1}^{m} \left(t_{hj} \times \sum_{i=1}^{n} v_{ij} \times A_j \right), \quad (5)$$

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 [10]. 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:

$$R = \sum_{i=1}^{g} R_i = \sum_{i=1}^{g} p_i \times T_i . \quad (6)$$

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:

$$L = \sum_{i=1}^{l} L_i . \quad (7)$$

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.

Комплекс таких мероприятий, организационных и технических, называется мероприятиями по внедрению средств защиты информации (СЗИ). Каждое мероприятие из СЗИ будет оказывать определенное влияние на совокупность угроз. Составим матрицу СЗИ с учетом применения требований законодательства L.

ТАБЛИЦА III МАТРИЦА ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА

	L_1	L_2	…	L_l
T_1	l_{11}	l_{12}	…	l_{1l}
T_2	l_{21}	l_{22}	…	l_{2l}
…	…	…	…	…
T_q	l_{q1}	l_{q2}	…	l_{ql}

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

$$T_h^{'} = \sum_{i=1}^{l} l_{hi} \times T_h , \quad (8)$$

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 [11] исходя из реализованных мер с учетом обновленных величин от реализации угроз $T_h^{'}$. С учетом этих мероприятий итоговая матрица мер СЗИ будет выглядеть так:

ТАБЛИЦА IV МАТРИЦА МЕР СЗИ

	D_1	D_2	…	D_l
$T_1^{'}$	d_{11}	d_{12}	…	d_{1l}
$T_2^{'}$	d_{21}	d_{22}	…	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:

$$T_h^{''} = \sum_{i=1}^{l} d_{hi} \times T_h^{'} , \quad (9)$$

где d_{hi} – воздействие СЗИ на угрозу $T_h^{'}$.

Соответственно меняется и оценочная величина риска $R_h^{''}$.

Для выбора конкретной технологии моделирования защиты АСУ ТП в первую очередь будем использовать формализованную структуру компонентов и связей АСУ ТП (1-3), множества атрибутов для оценки риска (4-9) 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 АСУ ТП 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 наиболее подходящей математической моделью будет являться обобщенная модель ИБ АСУ ТП типового газодобывающего предприятия вида:

$$M = \{C,S,A,T,V,P,D,R,L\}, \quad (10)$$

где C – множество компонентов системы;

S – множество типов связи между всеми компонентами;

A – множество стоимостей всех активов организации;

T – множество угроз;

$V_i = \{v_1,\ldots,v_h\}$ – множество уязвимостей угрозы T_i;

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.

III. 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 (10) 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.

Список литературы

[1] Сердцева А.В. Развитие автоматизированных систем управления технологическими процессами // Вестник УлГТУ. 2016. № 3(75). С. 58-61.

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

[3] 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.

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

[5] 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.

[6] Захаров А.А., Римша А.С., Харченко А.М., Зулькарнеев И.Р. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия // Вестник УрФО. Безопасность в информационной сфере. 2017. № 3(25). С. 24–33.

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

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

[9] Пищик Б.Н. Безопасность АСУ ТП // ЖВТ. 2013. № 5. С. 170-175.

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

[11] Римша А.С. К вопросу об информационной безопасности автоматизированных систем управления технологическими процессами газодобывающего предприятия // Сборник тезисов докладов: Вторая Арктическая совместная науч.-практ. конф., Новый Уренгой, 16-19 мая 2018 / ООО «Газпром добыча Уренгой» и «Газпром добыча Ямбург», 2018. С. 84-85.