www.volsu.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
В БЕЗОПАСНОСТИ И ТЕЛЕКОММУНИКАЦИЯХ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.4.3

УДК 004.942
ББК 32.971.35

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент,
кафедра информационной безопасности,
Волгоградский государственный университет
babenko.aleksey@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Андрей Александрович Вдовкин

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-231_275782@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Проанализированы результаты работ в области защиты АСУ ТП. Определены архитектура и функции АСУ ТП, влияющие на их безопасность. Рассмотрены угрозы ИБ АСУ ТП. Приведена модель угроз безопасности АСУ ТП. Представлена функциональная модель программного комплекса, предназначенного для оценки уровня риска ИБ в АСУ ТП. Описан программный комплекс оценки риска ИБ АСУ ТП. Приведены результаты экспериментальных исследований с помощью разработанной модели.

Ключевые слова: защита информации, оценка рисков, методы оценки рисков, АСУ ТП, контрмера, угроза, нарушитель.

Введение

В современном мире, где информационные технологии являются неотъемлемой частью бизнес-процессов, обеспечение безопасности информации становится все более важной задачей. Особенно это касается АСУ ТП, которые играют особенную роль в производстве и предоставлении услуг. Риски ИБ в таких системах могут привести к серьезным последствиям, включая потерю конфиденциальности, целостности и доступности данных, а также к возможным финансовым и репутационным потерям.

Для уменьшения рисков ИБ в АСУ ТП используются специализированные программные комплексы, которые помогают оценить и управлять рисками. В данной работе рассмотрена разработка программного комплекса оценки рисков ИБ АСУ ТП, его функциональные возможности и применение в реальной среде.

Теоретической базой для проведения исследования послужили труды авторов Т.С. Петрищева, В.Б. Кравченко, П.В. Зиновьев, И.Н. Селютин, С.В. Кирсанов, А.А. Бабенко и нормативно-правовые акты РФ [2; 3; 5; 6; 8].

Анализ АСУ ТП

Объекты атак выбраны в соответствии со статистикой атак на АСУ ТП [7], где атаки на производство составляют 31 %, а на отрасль нефти и газа 29,8 % (рис. 1).

В качестве объектов исследования выбраны:

1. АСУ ТП компрессорного цеха (АСУ ГПА, как часть системы компрессорного цеха).
2. АСУ аппаратов воздушного охлаждения газа (АВО) компрессорного цеха.
3. АСУ комплекса производства битума (КПБ).

АСУ ГПА используется с целью обеспечения эффективного и бесперебойного функционирования газоперекачивающего агрегата. Она осуществляет полный контроль и управление технологическими параметрами, гарантируя оптимальный режим работы и предотвращая возможные отказы и поломки. АСУ ГПА выполняет функции автоматического регулирования, контроля и защиты, обеспечивая долгосрочную и надежную работу газоперекачивающего агрегата.

Аппаратный состав АСУ ГПА на рисунке 2.

АСУ АВО компрессорного цеха поддерживает требуемую температуру газа на выходе АВО и защищает теплообменные трубы от гидратообразования. Аппаратный состав АСУ АВО компрессорного цеха представлен на рисунке 3.

Спроектируем и представим аппаратный состав АСУ комплекса производства битума (КПБ) на рисунке 4.

Анализ угроз ИБ АСУ ТП

Алгоритм нахождения угроз АСУ ТП состоит из следующих действий:

1. Выбор негативных последствий.
2. Выбор групп угроз.
3. Выбор объектов воздействия.

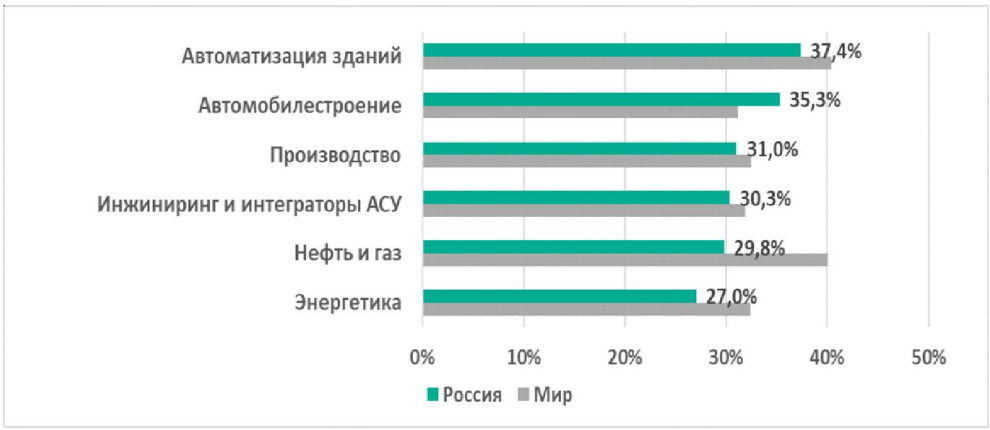

Рис. 1. Статистика атак на АСУ ТП

Уровень 4: Диспетчерский уровень	**АРМ диспетчера**	**Стойки УПИ (1-3 шт.)**	**Диспетчерский пульт (основной и запасной)**		**ПЭВМ сети цеха**
Уровень 3: Уровень систем автоматического управления	**Шкафы контроля технологических параметров**				
Уровень 2: Уровень контроллеров	**Программируемые логические контроллеры**				
Уровень 1: Датчики, исполнительные механизмы и преобразователи информации	**Датчики давления**	**Сигнализаторы давления**	**Преобразователи температуры**	**Датчики уровня**	**Сигнализаторы уровня**
Объекты управления	**Газотурбинный двигатель авиационного типа**				
	Модульные аппараты воздушного охлаждения (АВО) газа				
	Системы автономного обогрева ГПА				
	Блок подготовки топливного газа				

Рис. 2. Общая функциональная схема АСУ ГПА

Уровень 4: Диспетчерский уровень	**АРМ оператора**			
Уровень 3: Уровень систем автоматического управления	**Шкаф управления (технологический пульт)**			
	Шкафы стартеров плавного пуска и допускового контроля сопротивления изоляции двигателей			
	Шкафы НКУ			
Уровень 2: Уровень контроллеров	**Программируемые логические контроллеры**			
Уровень 1: Датчики, исполнительные механизмы и преобразователи информации	**Датчики температуры газа**	**Датчики температуры воздуха**	**Датчики положения кранов**	**Датчики давления**
Объекты управления	**Вентиляторы (6 штук)**			
	Жалюзи (12 штук)			
	Посты местного управления двигателями вентиляторов			
	Цифровая аппаратура контроля вибрации			
	Дожимная компрессорная станция			

Рис. 3. Общая функциональная схема АСУ

Уровень 4: Диспетчерский уровень	**АРМ Оператора**			
Уровень 3: Уровень систем автоматического управления	**Шкаф контроллеров и сетевого оборудования**	**Шкафы контроля технологических параметров**	**Шкаф управления отсечными клапанами**	**Щит силового управления**
Уровень 2: Уровень контроллеров	**Программируемые логические контроллеры**			
Уровень 1: Датчики, исполнительные механизмы и преобразователи информации	**Датчики температуры**	**Датчики давления**	**Датчики положения (сигнализаторы конечных положений)**	**Расходомеры жидкостей газов и взвесей**
Объекты управления	**Клапаны регулирующие**			
	Клапаны отсечные			
	Электроприводы ИМ-насосов, вентиляторов АВО, воздуходувок, шибера			
	Воздушные компрессоры			
	Стояки налива битума в авто- и ж/д цистерны			

Рис. 4. Общая функциональная схема АСУ КПБ

4. Выбор компонентов объектов воздействия.

5. Выбор уровня возможного нарушителя.

6. Получение списка угроз для рассматриваемых АСУ ТП.

Используя алгоритм нахождения угроз и списки компонентов, а также результаты формализованной модели формирования перечня угроз ФСТЭК составим программу которая будет являться частью экспериментов № 1–3. Для выбора объектов воздействия и негативных последствий воспользуемся статистикой [1] (рис. 5, 6).

Значения, используемые для получения списка угроз, представлены в таблице 1.

Модель нарушителя на объекты АСУ ТП, отражающая различные уровни их возможностей, представлена в таблице 2.

Для защиты от таких угроз необходимо принимать меры по обеспечению безопасности промышленных систем и устройств, а также обучать персонал вопросам ИБ.

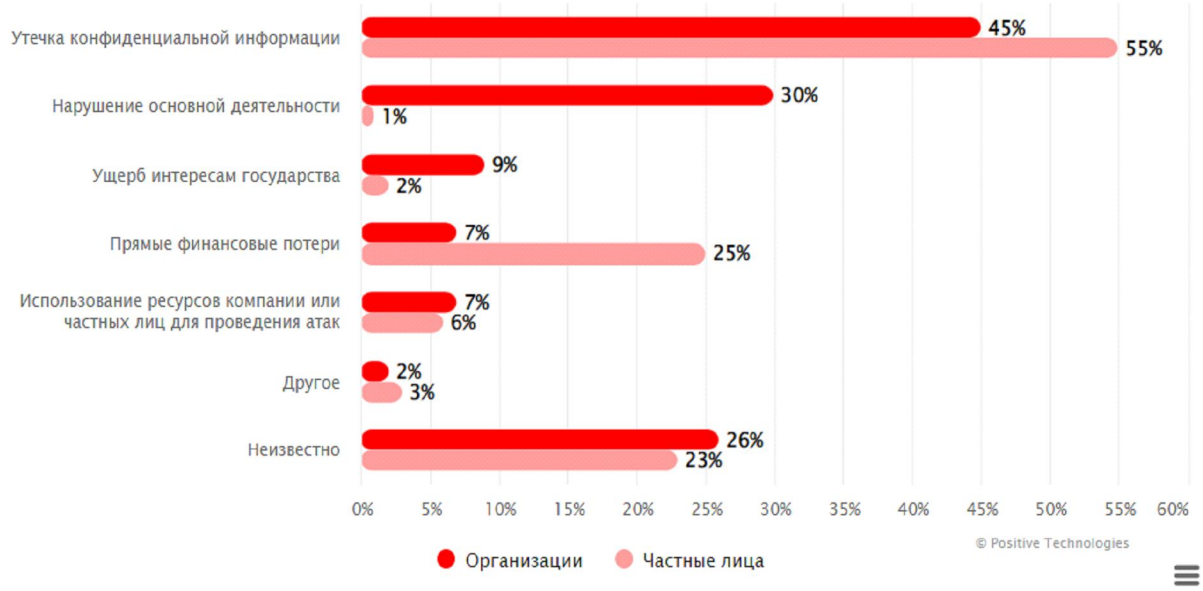

Рис. 5. Последствия атак злоумышленников (доля атак)

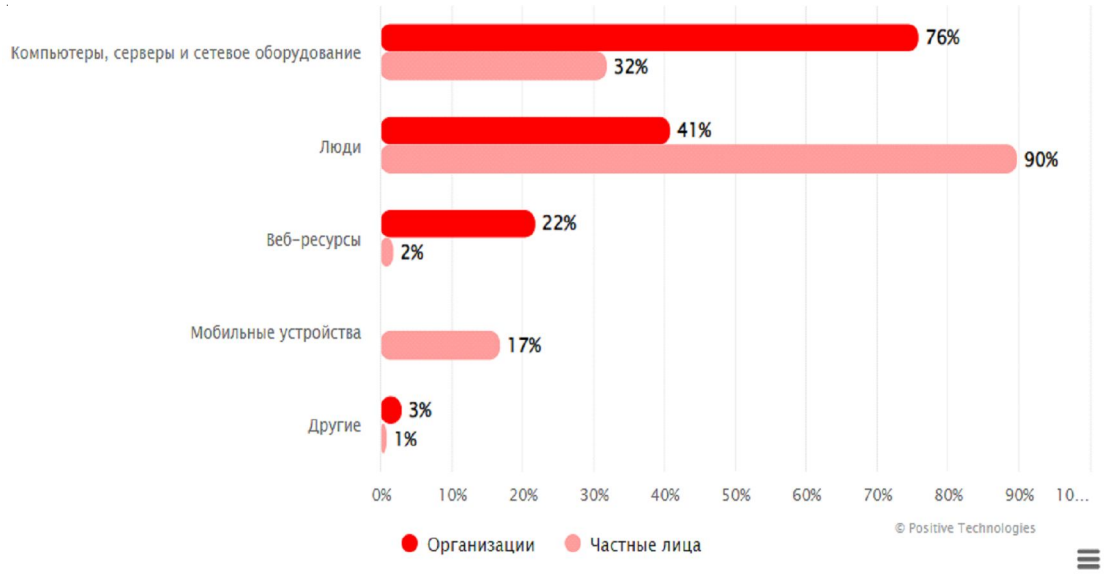

Рис. 6. Объекты атак

Сравнение подходов анализа рисков

Для выбора наилучшего проведен сравнительный анализ подходов для анализа рисков ИБ АСУ ТП (табл. 3).

По результатам анализа выбран метод CRAMM как наилучший. Важно отметить, что большинство характеристик, представленных в рассмотренных методах анализа рисков (см. табл. 3), базируются на качественных оценках, что снижает их эффективность. CRAMM способен оценивать риски для отдельных компонентов системы, но не учитывает их воздействие на систему в целом. Отметим, что во всех подходах при проведении оценки рисков не уделяется должного внимания негативным последствиям атак с использованием набора уязвимостей компьютерной безопасности, что является важной особенностью для АСУ ТП. Поэтому существует необходимость в разработке оригинальной методики расчета оценки риска ИБ для АСУ ТП.

Таблица 1

Классификация угроз АСУ ТП

Список компонентов	Объект атаки		
	Объект атаки № 1 (АСУ ГПА)	Объект атаки № 2 (АСУ АВО)	Объект атаки № 3 (АСУ КПБ)
Отрицательные последствия	1) потеря клиентов и поставщиков; 2) вредные воздействия на окружающую среду; 3) нарушение штатного режима функционирования АСУ ТП	1) недополучение прогнозируемой прибыли; 2) необходимость незапланированных затрат на восстановление деятельности; 3) нарушение штатного режима функционирования АСУ ТП	1) необходимость незапланированных затрат на закупку товаров, работ или услуг; 2) нарушение штатного режима функционирования АСУ ТП; 3) неспособность выполнения договорных обязательств
Группы угроз	УБИ.2 УБИ.8	УБИ.1 УБИ.3 УБИ.11	УБИ.6 УБИ.8
Объекты воздействия	1) автоматизированное рабочее место; 2) активное сетевое оборудование; 3) обеспечивающие системы	1) автоматизированное рабочее место; 2) устройство хранения данных; 3) физические линии связи	1) автоматизированное рабочее место; 2) обеспечивающие системы; 3) средства защиты информации

Таблица 2

Модель нарушителя

Уровень возможностей нарушителей	Средние возможности	Базовые (повышенные) возможности	Средние возможности
Список возможных угроз АСУ ТП (УБИ)	2.1.18. Несанкционированный доступ к АРМ за счет использования недостатков механизмов разграничения доступа	1.1.1. Утечка информации, обрабатываемой на АРМ, за счет эксплуатации уязвимостей	6.1.15. Вызов отказа в обслуживании АРМ за счет шифрования данных
	8.1.1. Нарушение работоспособности АРМ за счет эксплуатации уязвимостей	3.4.1. Несанкционированные искажения компонентов устройства хранения данных за счет эксплуатации уязвимостей	8.7.1. Нарушение работоспособности обеспечивающих систем за счет эксплуатации уязвимостей
	8.6.18. Нарушение работоспособности активного сет. оборудования за счет использования недостатков механизмов разграничения доступа	11.1.18. Несанкционированный массовый сбор информации с АРМ за счет использования недостатков механизмов разграничения доступа	8.9.18. Нарушение работоспособности СЗИ за счет использования недостатков механизмов разграничения доступа

Таблица 3

Сравнение подходов анализа рисков ИБ АСУ ТП

Методы оценки	Критерии			
	Анализ угроз с произвольными параметрами	Учет возможного ущерба и вероятности возникновения угрозы	Учет негативных последствий, связанных с группой уязвимостей	Взаимосвязь масштаба ущерба при реализации угрозы с иерархией активов
Имитационное моделирование и вероятность исполнения	Да	Да	Да	Да
CRAMM	Да	Да	Да	Да
FRAP	Да	Да	Нет	Нет
RiskWatch	Нет	Да	Да	Да
OCTAVE	Да	Нет	Да	Нет

Разработка функциональной модели программного комплекса оценки рисков ИБ АСУ ТП

Функциональная модель выполнена в соответствии с методологией IDEF0. Контекстная IDEF0-диаграма оценки рисков ИБ АСУ ТП представлена на рисунке 7.

В функциональном блоке «Оценка рисков ИБ АСУ ТП» заданы:

1. Входные данные – уровень нарушителя, группы угроз, негативные последствия, состав АСУ ТП, методы защиты.

2. Управляющая информация, в качестве которой выступает стандарт по управлению рисками ИБ CRAMM версии 5.1, приказы ФСТЭК РФ № 31, 235 и 239, ГОСТ Р ИСО/МЭК ТО 15446-2008, экспертная оценка.

3. Механизмами оценки рисков ИБ АСУ ТП, являются эксперт и программный комплекс.

4. Результат данных воздействий – риск ИБ АСУ ТП.

Декомпозиция функционального блока «оценки риска ИБ АСУ ТП» представлена на рисунке 8.

Функциональная модель позволила разработать программный комплекс оценки рисков ИБ АСУ ТП.

Проведение экспериментальных исследований

Определим угрозы для АСУ ТП с помощью разработанного программного комплекса (см. рис. 9, 10).

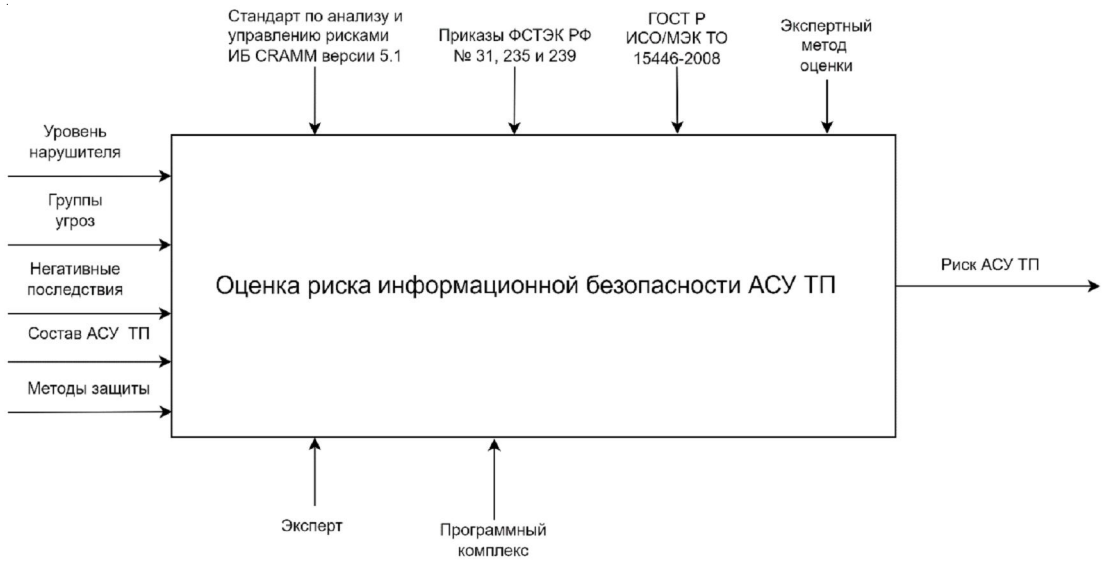

Рис. 7. Контекстная IDEF0-диаграмма оценки рисков ИБ АСУ ТП

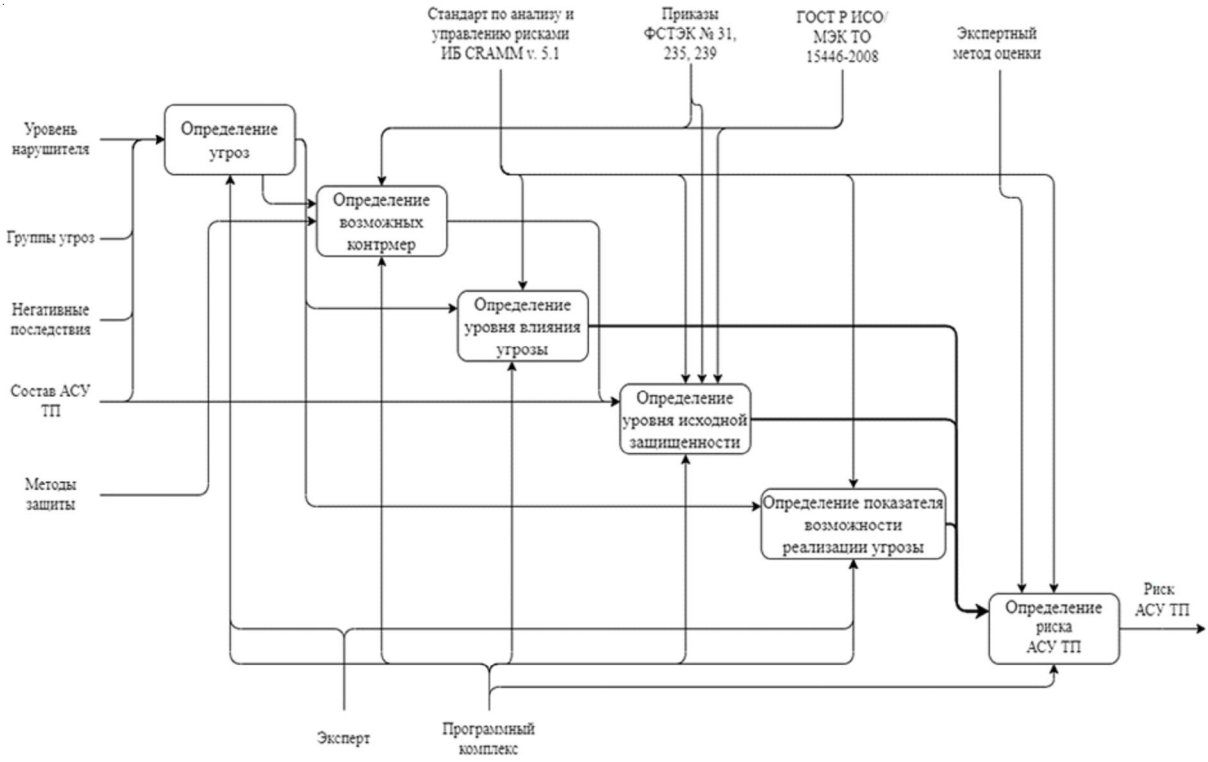

Рис. 8. Декомпозиция функционального блока «оценки рисков ИБ АСУ ТП»

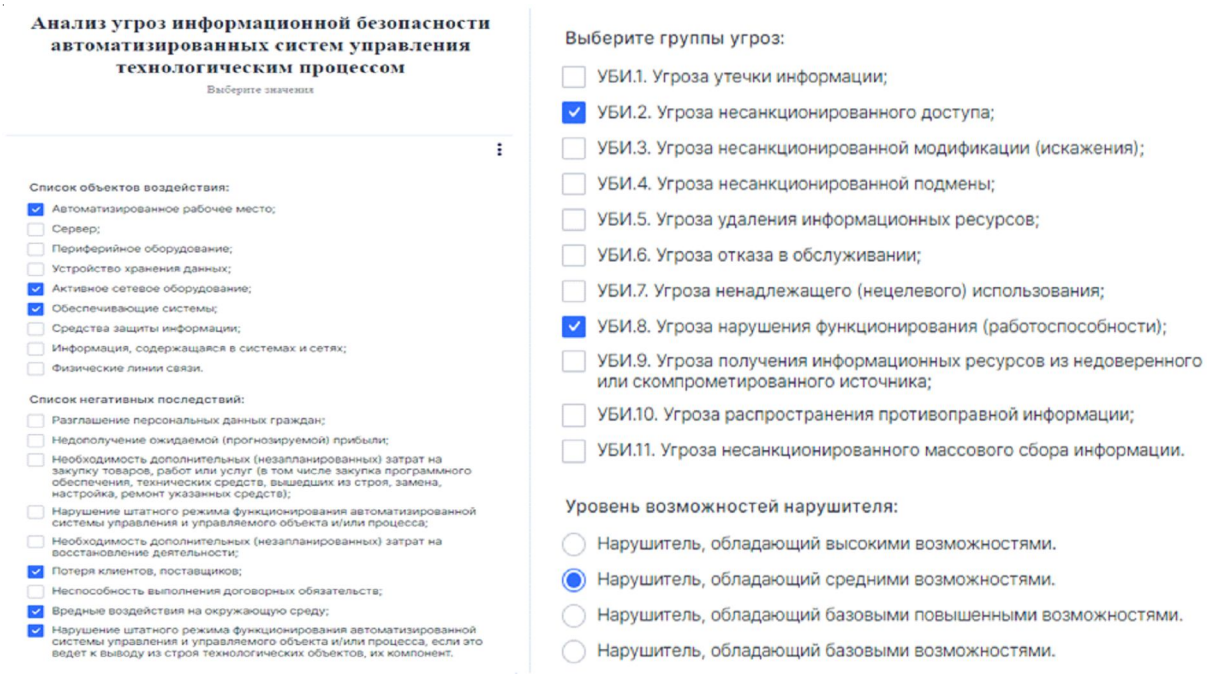

Рис. 9. Начальные параметры для получения перечня возможных угроз

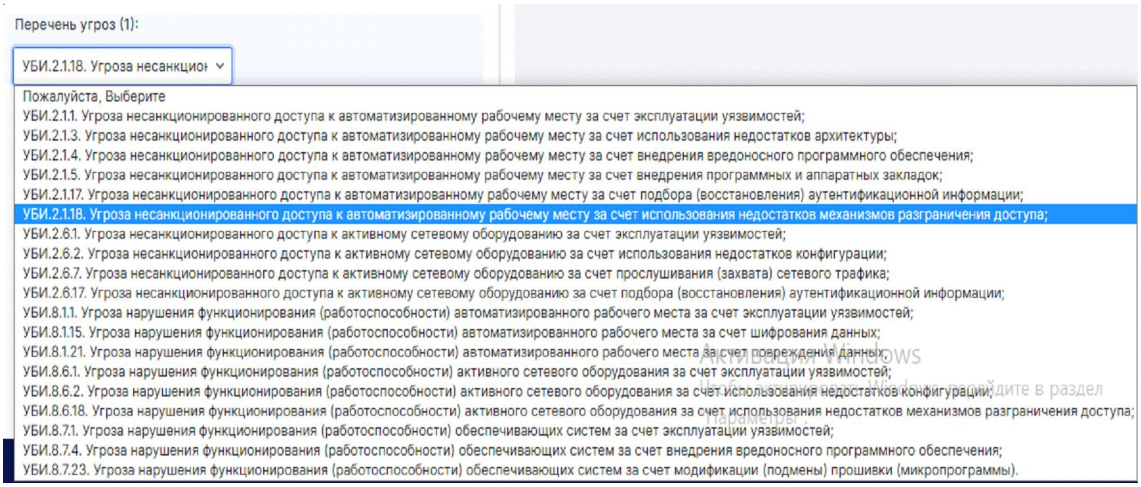

Рис. 10. Перечень возможных УБИ для АСУ ТП ГПА

В ходе экспериментального исследования было обнаружено 19 потенциальных угроз для АСУ ГПА. Для последующего этапа исследования были выбраны следующие информационные угрозы безопасности: УБИ 2.1.18, УБИ 8.1.1, УБИ 8.6.18.

Далее, задаем значения параметров для определения базовой оценки угрозы и уровня опасности (рис. 11).

В ходе выполнения программы рассчитан показатель уровня угрозы ИБ АСУ ТП, который выделен красным цветом на рисунке 11. Далее (рис. 12) определяется значения вероятности реализации и ущерба для угрозы УБИ 8.1.1.

В программу добавлен набор контрмер, и для каждой из них будет задана оценка веса конфиденциальности, целостности и доступности. Важно отметить, что сумма этих трех весов для каждой контрмеры не должна превышать 100 (рис. 13).

После внедрения контрмер произойдут изменения в оценке риска, оценке исходного уровня безопасности и возможности реализации угрозы. Это позволит нам отслеживать исходный уровень безопасности АСУ ТП, уровень риска, а также определить необходимые контрмеры для достижения желаемого уровня безопасности АСУ ТП и приемлемого уровня риска. На примере угрозы УБИ 8.1.1 был достигнут желаемый уровень безопасности и приемлемый уровень риска, что представлено на рисунке 14.

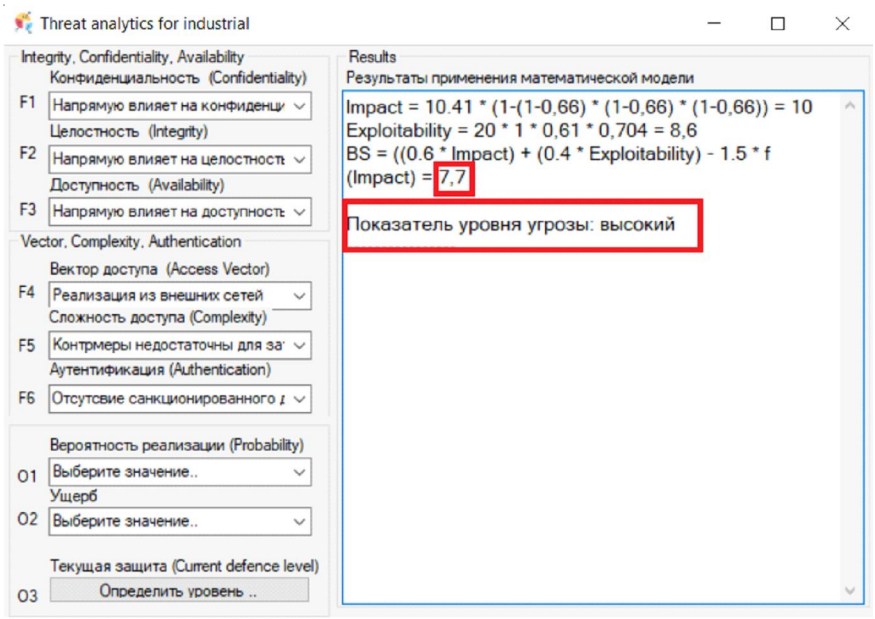

Рис. 11. Оценка угрозы и уровня опасности

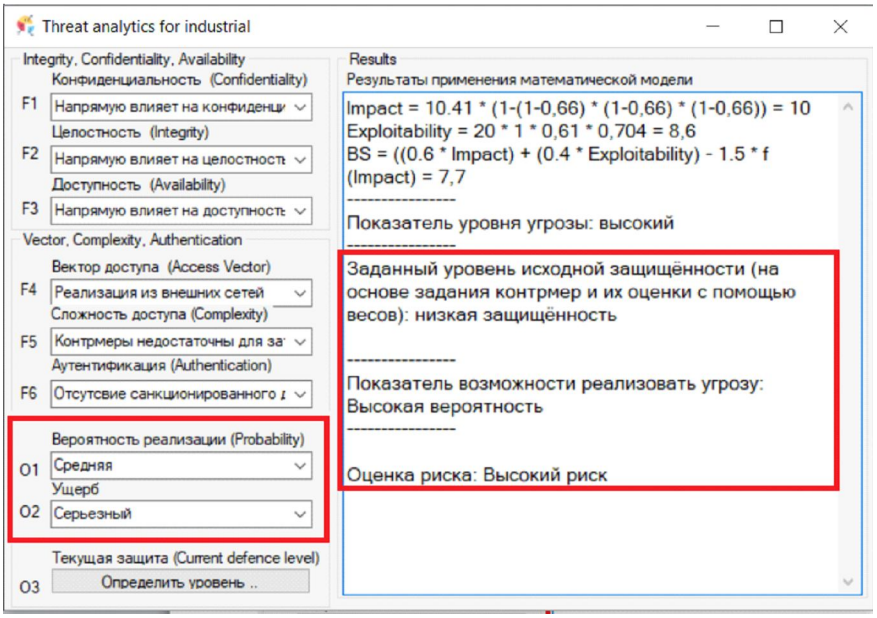

Рис. 12. Определение значения ущерба и вероятности реализации угрозы

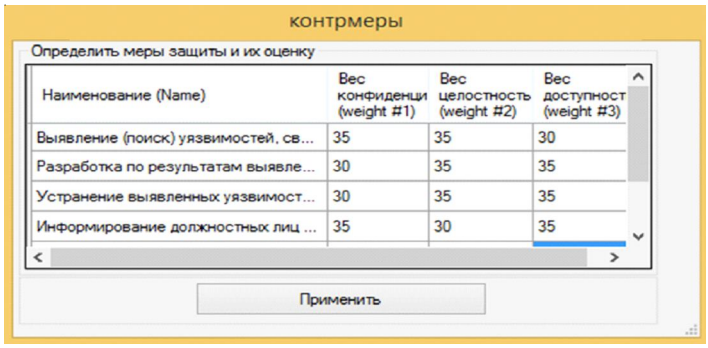

Рис. 13. Добавление контрмер

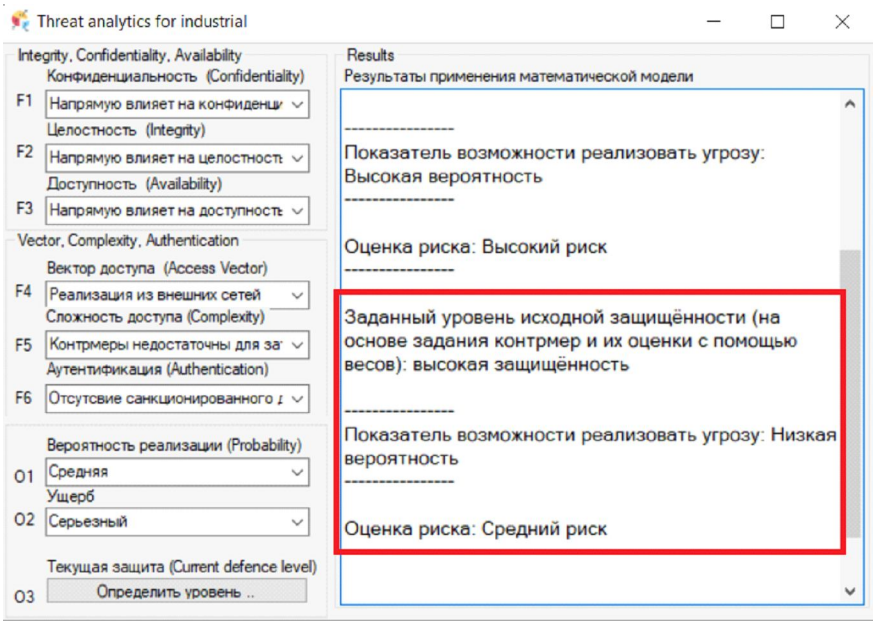

Рис. 14. Оценка уровня исходной защищенности, показателя возможности реализовать угрозу и уровня риска АСУ ТП после добавления контрмер

Экспериментально проверен разработанный метод оценки риска ИБ АСУ ТП. Для этого использовались предварительные оценки, сформированные экспертами на основе БДУ ФСТЭК РФ [4]. При разработке программы был использован комбинаторный подход, учитывающий все преимущества и недостатки методов оценки рисков АСУ ТП. Разработанный программный комплекс позволяет оценивать риски и предоставлять рекомендации по их устранению или нейтрализации, что обеспечивает эффективную защиту от потенциальных угроз ИБ АСУ ТП. Так уровень риска АСУ ТП ГПА снижен на 50 %, АСУ ТП комплекса производства битума на 30 %, АСУ ТП аппаратов воздушного охлаждения газа компрессорного цеха на 60 % в результате обоснованного определения состава системы защиты (рис. 15).

Заключение

При разработке программы был использован комбинаторный подход, учитывающий все преимущества и недостатки существующих подходов оценки рисков ИБ АСУ ТП. Программный комплекс предоставляет рекомендации по устранению или нейтрализации выявленных рисков, что обеспечивает эффективную защиту от потенциальных угроз ИБ АСУ ТП.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: I квартал 2022 года // Лидер результативной кибербезопасности. – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/. – Загл. с экрана.

2. Бабенко, А. А. Алгоритм оценки риска информационной безопасности автоматизированной системы управления технологическими процессами нефтегазовой отрасли / А. А. Бабенко, А. А. Вдовкин // Перспективные информационные технологии (ПИТ 2022) : тр. Междунар. науч.-техн. конф. – Самара: Изд-во Самар. науч. центра РАН, 2022. – С. 105–108.

3. Бабенко, А. А. Оценка риска информационной безопасности автоматизированной системы управления технологическим процессом / А. А. Бабенко, Д. А. Магомедов // Перспективные информационные технологии (ПИТ 2021) : тр. Междунар. науч.-техн. конф. – Самара: Изд-во Самар. науч. центра РАН, 2021. – С. 140–145.

4. Банк данных угроз безопасности информации // БДУ – Уязвимости. – Электрон. текстовые дан. – Режим доступа: https://bdu.fstec.ru/vul. – Загл. с экрана.

5. Кирсанов, С. В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли / С. В. Кирсанов // Доклады ТУСУРа. – 2013. – № 2 (28). – С. 112–115.

6. Кравченко, В. Б. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении : учеб. пособие / В. Б. Кравченко, П. В. Зиновьев, И. Н. Селютин. – М. : Академия, 2018. – 304 с.

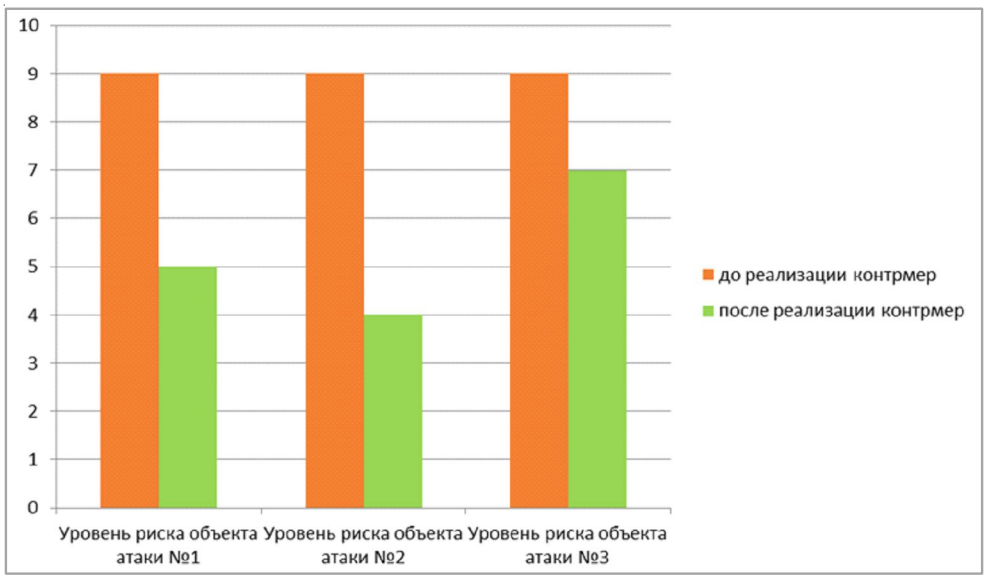

Рис. 15. Диаграмма уровня риска ИБ АСУ ТП:

1 – ГПА; *2* – комплекса производства битума; *3* – аппаратов воздушного охлаждения газа компрессорного цеха

7. Ландшафт угроз для систем промышленной автоматизации в России // Kaspersky ICS CERT. – Электрон. текстовые дан. – Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/. – Загл. с экрана.

8. Петрищева, Т. С. Оценка безопасности автоматизированной системы управления технологическими процессами нефтегазовой отрасли / Т. С. Петрищева, А. А. Вдовкин // Безопасность в современном мире : материалы IV Всерос. науч.-практ. конф. – Волгоград : Изд-во Волгогр. ин-та управления – фил. РАНХиГС, 2022. – С. 363–367.

REFERENCES

1. Aktualnye kiberugrozy: I kvartal 2022 goda [Actual Cyber Threats: 1st Quarter 2022]. *Lider rezultativnoj kiberbezopasnosti* [Leader of Effective Cyber Security]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/

2. Babenko A.A., Vdovkin A.A. Algoritm ocenki riska informacionnoj bezopasnosti avtomatizirovannoj sistemy upravlenija tehnologicheskimi processami neftegazovoj otrasli [Algorithm of Information Security Risk Assessment of the Automated Control System of Technological Processes of Oil and Gas Industry]. *Perspektivnye informacionnye tehnologii (PIT 2022): tr. Mezhdunar. nauch.-tehn. konf.* [Perspective Information Technologies (PIT 2022). Proceedings of the International Scientific and Technical Conference]. Samara, Izd-vo Samar. nauch. tsentra RAN, 2022, pp. 105-108.

3. Babenko A.A., Magomedov D.A. Ocenka riska informacionnoj bezopasnosti avtomatizirovannoj sistemy upravlenija tehnologicheskim processom [Information Security Risk Assessment of the Automated Process Control System]. *Perspektivnye informacionnye tehnologii (PIT 2021): tr. Mezhdunar. nauch.-tehn. konf.* [Perspective Information Technologies (PIT 2021). Proceedings of the International Scientific and Technical Conference]. Samara, Izd-vo Samar. nauch. tsentra RAN, 2021, pp. 140-145.

4. Bank dannyh ugroz bezopasnosti informacii [Databank of Information Security Threats]. *BDU – Ujazvimosti* [BDU – Vulnerabilities]. URL: https://bdu.fstec.ru/vul

5. Kirsanov S.V. Metod ocenki ugroz informacionnoj bezopasnosti ASU TP gazovoj otrasli [Method for Assessing Threats to Information Security of the ACS TP of the Gas Industry]. *Doklady TUSURa* [Reports of TUSUR], 2013, no. 2 (28), pp. 112-115.

6. Kravchenko V.B., Zinovyev P.V., Selyutin I.N. *Ekspluatacija avtomatizirovannyh (informacionnyh) sistem v zashhishhjonnom ispolnenii: ucheb. posobie* [Operation of Automated (Information) Systems in a Protected Version. Textbook]. Moscow, Akademiya Publ., 2018. 304 p.

7. Landshaft ugroz dlja sistem promyshlennoj avtomatizacii v Rossii [Threat Landscape for Industrial Automation Systems in Russia]. *Kaspersky ICS CERT*. URL: https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/

8. Petrishcheva T.S., Vdovkin A.A. Ocenka bezopasnosti avtomatizirovannoj sistemy upravlenija tehnologicheskimi processami neftegazovoj otrasli [Safety Assessment of the Automated Control System of Technological Processes of Oil and Gas Industry]. *Bezopasnost v sovremennom mire: materialy IV Vseros. nauch.-prakt. konf.* [Safety in the Modern World. Proceedings of the 4th All-Russian Scientific-Practical Conference]. Volgograd, Izd-vo Volgogr. in-ta upravleniya – fil. RANKhiGS, 2022, pp. 363-367.

DEVELOPMENT OF A SOFTWARE COMPLEX FOR EVALUATING INFORMATION SECURITY RISKS OF AN AUTOMATED PROCESS CONTROL SYSTEM

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Department of Information Security,
Volgograd State University
babenko.aleksey@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Andrei A. Vdovkin

Student, Department of Information Security,
Volgograd State University
IBm-231_275782@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. In today's world, where information technology is an integral part of business processes, information security is becoming increasingly important. This is especially true for process control systems, which play a special role in production and service delivery. IS risks in such systems can lead to serious consequences, including loss of confidentiality, integrity, and availability of data, as well as possible financial and reputational losses.

To mitigate IS risks, specialized software packages are used to help assess and manage risks. The results of work in the field of protection for automated process control systems are presented. The architecture and functions of automated process control systems affecting their security have been defined. Information security threats to automated process control systems have been examined. A security threat model for automated process control systems has been provided. A functional model of a software complex for assessing the risk of information security in automated process control systems is presented. The software complex for assessing the risk of information security in automated process control systems is described. The results of experimental research using the developed model are provided.

Key words: information security, risk assessment, methods of risk assessment, automated process control system, countermeasure, security threat, intruder.