ISSN 2225-9309 (Print)
2024. № 1 (30). С. 5–9
Молодежный Вестник УГАТУ
http://journal.ugatu.su

ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.65

ПОДХОД К АВТОМАТИЗАЦИИ ПРОЦЕССА ВЫБОРА ПРОГРАММНОГО СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Д. С. Алексеева[1], Н. А. Кононов[2]

[1] ads.stat@mail.ru, [2] knnv.nkt@gmail.com

[1, 2] ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. В представленной статье рассматривается вопрос выбора программного средства защиты информации. Рассматриваются виды сертифицированных программных средств. Предлагается подход к автоматизации процесса выбора программного средства защиты информации.

Ключевые слова: информационная безопасность; автоматизация; динамическая модель; современные подходы к ИБ.

ПОДХОД К АВТОМАТИЗАЦИИ ПРОЦЕССА ВЫБОРА ПРОГРАММНОГО СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Известно, что информационная безопасность является наиболее критически важной сферой деятельности любой организации, компании или государства. Защита информации от несанкционированного доступа и утечек является необходимой для обеспечения конфиденциальности, целостности и доступности информации.

Нарушение информационной безопасности может привести к многомиллионным потерям, как финансовым, так и репутационным. Утечка конфиденциальной информации может повлечь за собой серьезные последствия для безопасности государства и национальных интересов.

Важность информационной безопасности также связана с ростом использования цифровых технологий и интернета, что делает информацию более уязвимой для кибератак и различных видов хакерских атак.

Защита информации является неотъемлемой частью успешного функционирования любой организации. Под комплексом мер можно понимать: оценка уязвимостей, разработка политики безопасности, обучение персонала, использование антивирусного программного обеспечения, использование средств шифрования, резервное копирование данных, мониторинг системы, мониторинг системы, аудит системы, сотрудничество с профессиональными организациями, регулярное обновление программного обеспечения.

Этот комплекс мер может включать в себя следующие шаги:

1. Оценка уязвимостей: проведение анализа рисков и оценка уязвимостей системы информационной безопасности.

2. Разработка политики безопасности: создание политики безопасности, которая определяет правила и процедуры для обеспечения безопасности информации.

3. Обучение персонала: обучение сотрудников организации правилам и процедурам безопасности информации.

4. Использование антивирусного программного обеспечения: установка и использование антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.

5. Использование средств шифрования: использование средств шифрования для защиты конфиденциальной информации.

6. Резервное копирование данных: создание резервных копий данных для защиты от потери информации.

7. Мониторинг системы: мониторинг системы информационной безопасности для обнаружения и предотвращения возможных угроз.

8. Аудит системы: проведение аудита системы информационной безопасности для выявления уязвимостей и ошибок.

9. Сотрудничество с профессиональными организациями: сотрудничество с профессиональными организациями для получения экспертной помощи в области информационной безопасности.

10. Регулярное обновление программного обеспечения: регулярное обновление программного обеспечения для устранения уязвимостей и обеспечения безопасности системы.

В рамках данной статьи предлагается подход по подбору программного средства защиты информации, входящего в реестр ФСТЭК.

В состав программных средств информационной безопасности входят:

Системы предотвращения вторжений (*Intrusion Prevention Systems - IPS*) —программные и аппаратные средства, предназначенные для обнаружения и предотвращения попыток несанкционированного доступа к конфиденциальным данным, повышения привилегий, использования уязвимостей программного обеспечения и вывода из строя компьютерных систем.

Межсетевые экраны нового поколения (*Next-Generation Firewall - NGFW*) — типовые межсетевые экраны с возможностью отслеживания состояния соединений.

Системы предотвращения распределённого отказа в обслуживании (*Distributed Denial of Service (DDoS) Protection* или *Anti-DDoS*) — это специализированные программно-аппаратные и программные средства, предназначенные для защиты веб-серверов/сайтов компании от распределённых атак типа «Отказ в обслуживании».

Антивирусное программное обеспечение – программное обеспечение для обнаружения компьютерных вирусов и нежелательных программ, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

А также программно–аппаратные комплексы в виде шлюзов информационной безопасности и систем предотвращения утечки данных.

Программные средства могут входить в состав программных комплексов.

При выборе каждого из вышеперечисленных средств защиты организациям рекомендуется обращаться к реестру сертифицированных средств ФСТЭК.

Выбор средств защиты имеет определенную специфику для каждой организации, так как информационная система, подлежащая защите. может принадлежать государственному учреждению или частной организации.

При разборе каждой организации специалист по защите информации вынужден повторять определенные операции при каждом подборе СЗИ для ИС.

Для увеличения эффективности предлагается ввести информационную систему, связанную с реестром ФСТЭК и позволяющую

Общий вид процесса выбора программных средств обеспечения информационной безопасности представлен на рис. 1 динамической моделью в нотации BPMN [2].

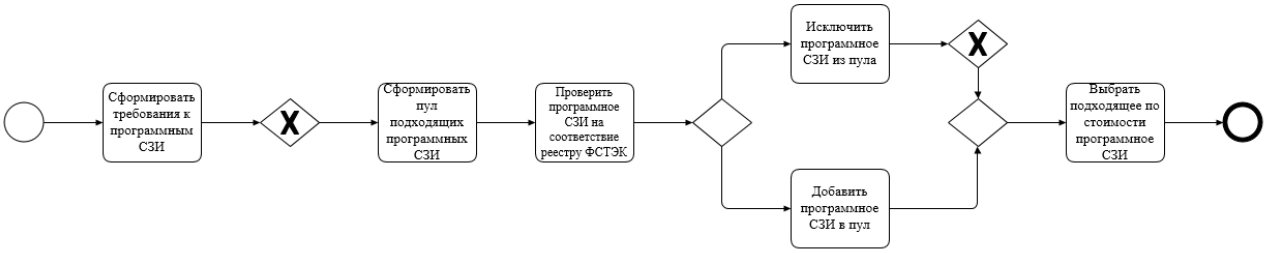

Рис. 1. Динамическая модель процесса в нотации *BPMN*.

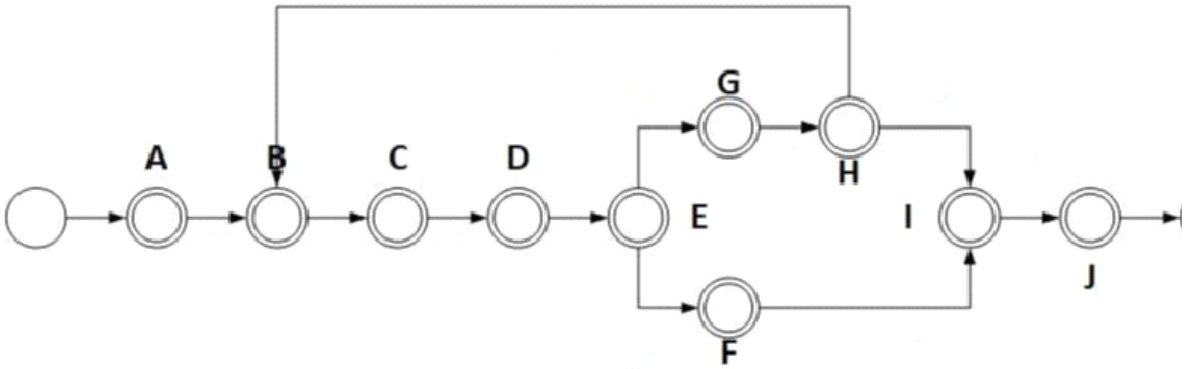

Рис. 2. Упрощенная модель.

Упрощая BPMN - модель с рис. 1 до модели, показанной на рис. 2, можно получить формулу 1, которая описывает процесс выбора программного средства обеспечения информационной безопасности, но более в общем виде.

$$P=A+C+D+E+F+I+J \quad (1)$$

P – Процесс выбора программного СЗИ;
A – Сформировать требования к программным СЗИ;
C – Сформировать пул подходящих программных СЗИ;
D – Проверить программное СЗИ на соответствие реестру ФСТЭК;
G – Исключить программное СЗИ из пула;
F – Добавить программное СЗИ в пул;
J – Выбрать подходящее по стоимости программное СЗИ.

Исходя из формулы, в среднем ручной выбор может занять до 530 минут (формула 2), что соответствует полноценному восьмичасовому рабочему дню.

$$P=180+240+60+5+5+40=530 \quad (2)$$

При внедрении информационной системы, позволяющей автоматизировать процесс выбора программного СЗИ (Рисунок 3) затраченное время может сократиться до 210 минут (формула 4).

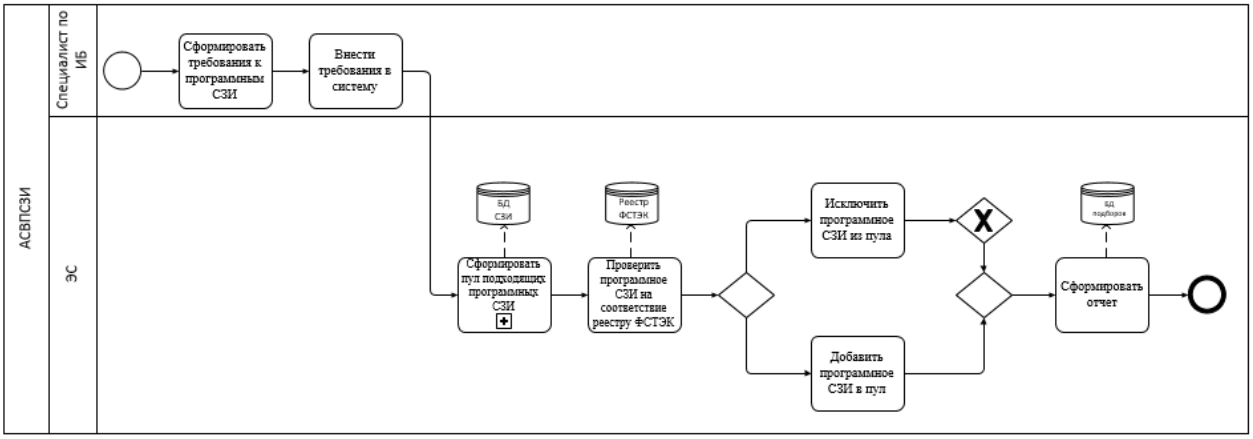

Рис. 3. *BPMN* – модель обозначенного процесса применением ИС.

Сокращение времени возможно рассчитать с помощью формулы 3, которая основана на рисунке 4. Результат представлен в виде формулы 4.

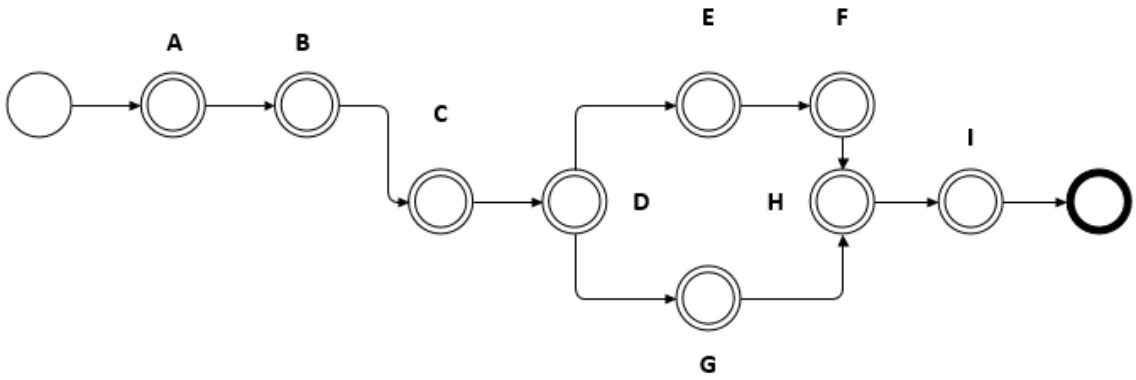

Рис. 4. Упрощенная *BPMN* – модель.

$$P=A+C+D+E+G+I \quad (3)$$

P – Процесс выбора программного СЗИ;
A – Сформировать требования к программным СЗИ;
B - Внести требования в систему;
C – Сформировать пул подходящих программных СЗИ;
D – Проверить программное СЗИ на соответствие реестру ФСТЭК;
E – Исключить программное СЗИ из пула;
G – Добавить программное СЗИ в пул;
I – Выбрать подходящее по стоимости программное СЗИ.

$$P=180+15+5+2+2+1+5=210 \quad (4)$$

Таким образом применение информационной системы позволяет специалисту по информационной безопасности принять решение по выбору средства защиты информации за 3,5 часа, тогда как при ручном подходе выбор может занять до 1 рабочего дня.

СПИСОК ЛИТЕРАТУРЫ

1. **Обеспечение** сетевой безопасности совместно с брокерами сетевых пакетов. Часть первая. Пассивные средства безопасности [Электронный ресурс]: https://dsol.ru/company/library/article-habr-3/ (Дата обращения 25.11.2021) [Ensuring network security in conjunction with network packet brokers. Part one. Passive safety measures]

2. **Балантер Б. И., Ханин М. А., Чернавский Д.С.** Введение в математическое моделирование патологических процессов; Наука - Москва, 2019. - 264 с. [B.I. Balanter, M.A. Khanin, D.S. Chernavsky. Introduction to mathematical modeling of pathological processes; Nauka Moscow, 2019. pp. 264]

3. **Государственный реестр** сертифицированных средств защиты информации [Электронный ресурс]: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (Дата обращения 25.11.2021). [The State Register of certified Information Security Tools].

4. **Шаньгин В. Ф.** Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). [V. F. Shangin. Information security of computer systems and networks: a textbook. Moscow : FORUM : INFRA-M, 2021. pp. 416 p.]

5. **«Критерии оценки доверенных компьютерных систем»** - стандарт / Министерство Обороны США, 1983 г.["Criteria for evaluating trusted computer systems" - standard / US Department of Defense, 1983]

ОБ АВТОРАХ

АЛЕКСЕЕВА Дарья Сергеевна, магистрант кафедры ВТиЗИ (УУНиТ, 2024).

КОНОНОВ Никита Алексеевич, магистрант кафедры АСУ (УУНиТ, 2024).

METADATA

Title: An approach to automating the process of selecting a software tool for information protection.

Authors: D.S. Alexeeva[1], N.A. Kononov[2]

Affiliation:

[1,2] Ufa University of Science and Technology (UUST), Russia.

Email: [1] ads.stat@mail.ru, [2] knnv.nkt@gmail.com

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 1 (30), pp. 5-9, 2024. ISSN 2225-9309 (Print).

Abstract: The presented article discusses the issue of choosing a software tool for information protection. The types of certified software tools are considered. An approach to automating the process of selecting a software tool for information protection is proposed.

Key words: information security; automation; dynamic model; modern approaches to information security.

About authors:

ALEKSEEVA Darya Sergeevna, master student of the Faculty. VTiZI (UUST, 2024)

KONONOV Nikita Alekseevich, master student of the Faculty of ASU (UUST, 2024).