DOI: 10.53403/9785951505460_542

ВОЗМОЖНЫЙ ПОДХОД К ОЦЕНКЕ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ (УЩЕРБА) ОТ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТНОШЕНИИ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Рычагов Кирилл Константинович (kkrychagov@vniief.ru), Дубровин Руслан Юрьевич, Булычев Роман Владимирович, Аннин Дмитрий Геннадьевич, Афонин Андрей Петрович, Жорин Вячеслав Викторович

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

С учетом складывающейся ситуации в стране и мире на фоне стремительного развития информационных технологий, как никогда актуальной становится задача обеспечения безопасности информации на всех этапах жизненного цикла автоматизированной системы (от разработки системы до ее вывода из эксплуатации).

Одним из ключевых этапов обеспечения защиты информации является моделирование угроз информационной безопасности, актуальных для автоматизированной системы (АС). При этом актуальность угрозы напрямую зависит от негативных последствий (ущерба), которые могут наступить при реализации угрозы. Поскольку существует необходимость корректного определения негативных последствий (ущерба) от реализации угроз безопасности информации, разработка подхода к оценке таких последствий является актуальной задачей.

Ключевые слова: оценка негативных последствий, показатели эффективности автоматизированных систем, угрозы безопасности информации

POSSIBLE APPROACH TO ASSESSING NEGATIVE CONSEQUENCES (DAMAGE) FROM IMPLEMENTATION OF INFORMATION SECURITY THREATS WITH REGARD TO THE PERFORMANCE INDICATORS OF AUTOMATED SYSTEMS IN PROTECTED PERFORMANCE

Rychagov Kirill Konstantinovich(kkrychagov@vniief.ru), Dubrovin Ruslan Yurievich, Bulychev Roman Vladimirovich, Annin Dmitry Gennadievich, Afonin Andrey Petrovich, Zhorin Vyacheslav Victorovich

FSUE «RFNC-VNIIEF», Sarov Nizhny Novgorod region

Taking into account the current situation in the country and in the world in the time of rapid development of information technologies, the problem of ensuring information security at all stages of the life cycle of the automated system (from system development to its decommissioning) becomes more urgent than ever.

One of the key stages of information protection is modeling of information security threats that are relevant to the automated system. At the same time, the relevance directly depends on negative consequences (damage) that may occur when the threat is realized. Since there is a need to determine negative consequences (damage) from implementation of information security threats correctly, development of an approach to assess these consequences is an urgent task.

Keywords: assessment of negative consequences, indicators of automated systems performance, information security threats.

Описание подхода

Для оценки негативных последствий (ущерба) от реализации угроз информационной безопасности предлагается подход, предполагающий последовательное выполнение следующих этапов:

1. Производится анализ перечня угроз безопасности информации (УБИ), приведенного в открытом банке ФСТЭК [1]. Из перечня УБИ исключаются неподходящие УБИ (с точки зрения назначения, функций, состава или архитектуры) рассматриваемой системы. Результатом будет являться перечень из оставшихся k УБИ.

2. Вводятся величины P_j (вероятность (возможность) реализации угрозы, где $j = 1, \ldots, k$), x_{ji} (степень негативного воздействия УБИ$_j$ на i-ый показатель эффективности системы, где $i = 1, \ldots, m$) и X_j (степень негативного воздействия УБИ$_j$ на показатели эффективности системы) и определяются для каждой из УБИ. Величины x_{ji} оцениваются следующим образом: если при реализации УБИ$_j$ осуществляется негативное влияние, незначительно воздействующее или не воздействующее на i-ый показатель эффективности, то x_{ji} – низкая степень, умеренно воздействующее – средняя степень, существенно воздействующее – высокая степень. Величинам X_j присваивается максимальное значение x_{ji}. Оценка величин P_j осуществляется в соответствии с табл. 1.

Решение о дальнейшем рассмотрении УБИ$_j$ принимается на основании полученных экспертных оценок в соответствии с табл. 2.

3. Оценивается степень возможных негативных последствий (ущерба) от реализации УБИ, определенных на этапе 2, в соответствии с табл. 3 – 9. Основными видами ущерба, которые могут возникнуть при реализации УБИ являются: экономический (финансовый) ущерб; социальный ущерб; политический ущерб; репутационный ущерб; ущерб в области обороны, безопасности и правопорядка; ущерб субъекту персональных данных; технологический ущерб.

Таблица 1

Оценка величин P_j

Частота возникновения возможности для реализации УБИ$_j$ / Мотивация предполагаемого нарушителя	Частота возникновения возможности для реализации УБИ$_j$ в «идеальных» условиях (при которых возможности предполагаемого нарушителя ограничены только уровнем его технической подготовки)		
	Не превышает 1 раза в 5 лет	Не превышает 1 раза в 1 год	Превышает 1 раз в 1 год
Отсутствует	Низкая	Низкая	Низкая
Может существовать	Низкая	Средняя	Высокая

Таблица 2

Принятие решение о дальнейшем рассмотрении УБИ$_j$

Вероятность (возможность) реализации угрозы, P_j	Степень негативного воздействия УБИ$_j$ на показатели эффективности АС, X_j		
	Низкая	Средняя	Высокая
Низкая	не рассматривается	не рассматривается	рассматривается
Средняя	не рассматривается	рассматривается	рассматривается
Высокая	рассматривается	рассматривается	рассматривается

Таблица 3

Степень экономического (финансового) ущерба

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен.
Низкая	• недополучение ожидаемой (прогнозируемой) прибыли; • потеря клиентов, поставщиков; • потеря конкурентного преимущества
Средняя	• потеря финансовых средств; • необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; • необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)
Высокая	• невозможность заключения договоров, соглашений; • необходимость дополнительных (незапланированных) затрат на восстановление деятельности

Таблица 4

Степень социального ущерба

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен
Низкая	• увеличение количества жалоб в органы государственной власти или органы местного самоуправления; • появление негативных публикаций в общедоступных источниках
Средняя	• организация пикетов, забастовок, митингов и других акций; • увольнения
Высокая	• угроза жизни или здоровью граждан; • прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения

Таблица 5

Степень политического ущерба

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен
Низкая	• нарушение выборного процесса
Средняя	• неспособность выполнения международных (двусторонних) договорных обязательств; • невозможность заключения международных (двусторонних) договоров, соглашений
Высокая	• создание предпосылок к обострению отношений в международных отношениях; • создание предпосылок к внутриполитическому кризису

Таблица 6

Степень репутационного ущерба

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен
Низкая	• нарушение деловой репутации; • снижение престижа
Средняя	• дискредитация работников; • неспособность выполнения договорных обязательств
Высокая	• нарушение законодательных и подзаконных актов; • утрата доверия

Таблица 7

Степень ущерба в области обороны, безопасности и правопорядка

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен.
Низкая	• нарушение общественного правопорядка; • неблагоприятное влияние на обеспечение общественного правопорядка
Средняя	• возможность потери или снижения уровня контроля за общественным правопорядком
Высокая	• создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка; • отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации

Таблица 8

Степень ущерба субъекту персональных данных

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен
Низкая	• моральный вред; • утрата репутации
Средняя	• финансовые или иные материальные потери физического лица; • вторжение в частную жизнь
Высокая	• создание угрозы здоровью; • создание угрозы личной безопасности

Таблица 9

Степень технологического ущерба

Степень ущерба	Возможные негативные последствия
Минимальная	ущерб не может быть оценен
Низкая	• необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)
Средняя	• простой АС или ее сегмента
Высокая	• невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); • принятие неправильных решений

Степени ущерба определяются для каждой из УБИ, полученных на этапе 2, в соответствии с возможными негативными последствиями, указанными в приложении 4 [2]. Итоговая степень ущерба для каждой УБИ определяется по максимальному полученному значению степени ущерба для всех основных видов ущерба. Результирующий перечень УБИ формируется из УБИ, имеющих итоговые степени ущерба – «высокая» или «средняя».

Пример реализации подхода

Рассмотрим на примере реализацию описанного подхода. Пусть имеется АС на базе автономной (взаимодействие с другими системами через «воздушный зазор») персональной электронно-вычислительной машины. В АС обрабатывается информация ограниченного доступа. Выберем в качестве примера показатели эффективности: надежность, производительность ($m = 2$).

1. Проанализируем перечень УБИ, приведенный в открытом банке ФСТЭК [1] и исключим неподходящие УБИ (в части назначения, функций, состава или архитектуры) рассматриваемой системы. Для простоты дополнительно сократим перечень УБИ до четырех угроз: угроза нарушения работы АС, вызванного обновлением используемого в ней программного обеспечения; угроза физического устаревания аппаратных компонентов; угроза некорректного использования функционала программного и аппаратного обеспечения; угроза подбора пароля Basic Input/Output System (далее – BIOS) ($k = 4$).

2. Определим наличие негативного влияния на показатели эффективности системы в результате реализации УБИ и уточним перечень УБИ, полученный на этапе 1. Для этого введем величины P_1 (вероятность реализации угрозы нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения), P_2 (вероятность реализации угрозы физического устаревания аппаратных компонентов), P_3 (вероятность реализации угрозы некорректного использования функционала программного и аппаратного обеспечения), P_4 (вероятность реализации угрозы подбора пароля BIOS), x_{11}, x_{21}, x_{31}, x_{41} (степени негативного воздействия УБИ, полученных на этапе 1, на надежность системы), x_{12}, x_{22}, x_{32}, x_{42} (степени негативного воздействия УБИ, полученных на этапе 1, на производительность системы) и X_1, X_2, X_3, X_4 (степени негативного воздействия УБИ, полученных на этапе 1, на надежность и производительность системы). Оценим вышеуказанные величины экспертным методом.

Реализация угрозы нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения может предполагать преднамеренную или неумышленную установку в системе обновлений программного обеспечения, в которых имеются критические ошибки, дефекты, уязвимости и прочее, что может умеренно повлиять на надежность и производительность рассматриваемой системы (x_{11}, x_{12} – средняя). Следовательно, для данной УБИ устанавливается средняя степень влияния на показатели эффективности (X_1 – средняя). Может иметь место финансовая мотивация со стороны третьих лиц. Частота возникновения возможности для реализации данной УБИ в «идеальных» условиях не превышает 1 раз в 1 год. Таким образом, для данной УБИ устанавливается средняя вероятность реализации (P_1 – средняя). Исходя из вышеперечисленного, принимается решение о дальнейшем рассмотрении данной УБИ.

Реализация угрозы физического устаревания аппаратных компонентов может предполагать преднамеренную или неумышленную халатность в части реализации установленных регламентов по обновлению аппаратных компонентов АС, что может существенно повлиять на надежность и производительность рассматриваемой системы (x_{21}, x_{22} – высокая). Следовательно, для данной УБИ устанавливается высокая степень влияния на показатели эффективности (X_2 – высокая). В случае преднамеренной халатности может иметь место финансовая мотивация со стороны третьих лиц. Частота возникновения возможности для реализации УБИ в «идеальных» условиях не превышает 1 раз в 1 год. Таким образом, для данной УБИ устанавливается средняя вероятность

реализации (P_2 – средняя). Исходя из вышеперечисленного, принимается решение о дальнейшем рассмотрении данной УБИ.

Реализация угрозы некорректного использования функционала программного и аппаратного обеспечения может сопровождаться негативным влиянием лишь незначительно воздействующим или не воздействующим на надежность и производительность рассматриваемой системы (x_{31}, x_{32} – низкая). Следовательно, для данной УБИ устанавливается низкая степень влияния на показатели эффективности (X_3 – низкая). Отсутствует мотивация для реализации УБИ. Частота возникновения возможности для реализации УБИ в «идеальных» условиях не превышает 1 раза в 5 лет. Таким образом, для УБИ устанавливается низкая вероятность реализации (P_3 – низкая). Исходя из вышеперечисленного, принимается решение далее не рассматривать данную УБИ.

Реализация угрозы подбора пароля BIOS может сопровождаться негативным влиянием лишь незначительно воздействующим или не воздействующим на надежность и производительность рассматриваемой системы (x_{41}, x_{42} – низкая). Следовательно, для данной УБИ устанавливается низкая степень влияния на показатели эффективности (X_4 – низкая). Может иметь место финансовая мотивация со стороны третьих лиц. Частота возникновения возможности для реализации УБИ в «идеальных» условиях превышает 1 раз в 1 год. Таким образом, для УБИ устанавливается высокая вероятность реализации (P_4 – высокая). Исходя из вышеперечисленного, принимается решение о дальнейшем рассмотрении данной УБИ.

В итоге уточненный перечень УБИ состоит из трех УБИ: угроза нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения; угроза физического устаревания аппаратных компонентов; угроза подбора пароля BIOS.

Результаты этапа 2 приведены в табл. 10.

3. Оценим степень возможных негативных последствий (ущерба) от реализации УБИ, определенных на этапе 2. Социальный ущерб, политический ущерб, ущерб в области обороны, безопасности и правопорядка и ущерб субъекту персональных данных не могут быть оценены, следовательно, для указанных видов ущерба устанавливаются минимальные степени ущерба. Результаты определения степени технологического ущерба приведены в табл. 11, репутационного ущерба – в табл. 12, экономического ущерба – в табл. 13.

В табл. 14 представлены результаты определения итоговой степени ущерба для каждой УБИ по максимальному полученному значению степени ущерба для всех видов ущерба. Результирующий перечень УБИ представлен двумя УБИ (угрозой нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения и угрозой физического устаревания апапаратных компонентов), имеющих итоговые степени ущерба – «средняя» и «высокая»

Таблица 10

Определение наличия негативного воздействия на показатели эффективности АС

№ п/п, j	Наименование УБИ	Степень негативного воздействия на показатель эффективности АС, x_{ji}		Степень негативного воздействия на показатели эффективности АС, X_j	Вероятность (возможность) реализации УБИ, P_j	Решение о дальнейшем рассмотрении УБИ
		Надежность	Производительность			
1	Угроза нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения	средняя	средняя	средняя	средняя	рассматривается
2	Угроза физического устаревания аппаратных компонентов	высокая	высокая	высокая	средняя	рассматривается
3	Угроза некорректного использования функционала программного и аппаратного обеспечения	низкая	низкая	низкая	низкая	не рассматривается
4	Угроза подбора пароля BIOS	низкая	низкая	низкая	высокая	рассматривается

Таблица 11

Степень технологического ущерба

Наименование УБИ	Возможные негативные последствия	Степень ущерба
Угроза нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения	• необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций); • простой АС или ее сегмента	Средняя
Угроза физического устаревания аппаратных компонентов	• необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций); • простой АС или ее сегмента; • невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	Высокая
Угроза подбора пароля BIOS	• необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	Низкая

Таблица 12

Степень репутационного ущерба

Наименование УБИ	Возможные негативные последствия	Степень ущерба
Угроза нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения	дискредитация работников	Средняя
Угроза физического устаревания аппаратных компонентов	• снижение престижа; неспособность выполнения договорных обязательств	Средняя
Угроза подбора пароля BIOS	• нарушение деловой репутации; • снижение престижа.	Низкая

Таблица 13

Степень экономического ущерба

Наименование УБИ	Возможные негативные последствия	Степень ущерба
Угроза нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения	• недополучение ожидаемой (прогнозируемой) прибыли; • необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)	Средняя
Угроза физического устаревания аппаратных компонентов	• недополучение ожидаемой (прогнозируемой) прибыли; • потеря клиентов, поставщиков; • потеря конкурентного преимущества; • потеря финансовых средств; • необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; • необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); • невозможность заключения договоров, соглашений; • необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Высокая
Угроза подбора пароля BIOS	ущерб не может быть оценен	Минимальная

Таблица 14

Результаты определения итоговой степени ущерба

Наименование УБИ	Степень ущерба							Итоговая степень ущерба
	экономического (финансового)	социального	политического	репутационного	в области обороны, безопасности и правопорядка	субъекту персональных данных	технологического	
Угроза нарушения работы автоматизированной системы, вызванного обновлением используемого в ней программного обеспечения	Средняя	Минимальная	Минимальная	Средняя	Минимальная	Минимальная	Средняя	Средняя
Угроза физического устаревания аппаратных компонентов	Высокая	Минимальная	Минимальная	Средняя	Минимальная	Минимальная	Высокая	Высокая
Угроза подбора пароля BIOS	Минимальная	Минимальная	Минимальная	Низкая	Минимальная	Минимальная	Низкая	Низкая

Заключение

Разработан подход к оценке негативных последствий (ущерба) от реализации угроз безопасности информации в отношении показателей эффективности автоматизированных систем в защищенном исполнении.

Выполнена оценка негативных последствий реализации УБИ на примере.

Полученные результаты (итоговый перечень УБИ и негативные последствия) могут быть использованы в дальнейшем при моделировании УБИ в соответствии с методикой [2].

Список литературы

1. Банк данных угроз безопасности информации. [Электронный ресурс]: [веб-сайт]. – Электрон. дан. – URL: https://bdu.fstec.ru/ (дата обращения 20.07.2022).

2. Методический документ. Методика оценки угроз безопасности информации. М: ФСТЭК России, 2021.