ПРИМЕНЕНИЕ МЕТОДОВ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ К ОЦЕНКЕ РИСКОВ НАРУШЕНИЯ КРИТИЧЕСКИ ВАЖНЫХ СВОЙСТВ ЗАЩИЩАЕМЫХ РЕСУРСОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Братченко А.И.[1], Бутусов И.В.[2], Кобелян А.М.[3], Романов А.А.[4]

Цель статьи: *разработка метода оценки рисков нарушения критически важных свойств защищаемых ресурсов с различными категориями важности в условиях высокой неопределенности.*

Метод: *моделирование распределения механизмов защиты по нейтрализуемым угрозам безопасности информации и применение методов теории нечетких для оценки рисков нарушения критически важных свойств.*

Полученный результат: *показано, что существующие модели систем защиты информации и методы оценки рисков нарушения критически важных свойств защищаемых ресурсов недостаточно полно отражают специфику систем защиты информации как сложных организационно-технических систем. Поведение таких систем отражает динамику слабоструктурированных процессов, характеризующихся высокой степенью неопределенности вследствие нестационарности, неточности и недостаточности наблюдений, нечеткости и нестабильности тенденций. Обоснована актуальность научной задачи оценки рисков нарушения критически важных свойств защищаемых ресурсов в условиях высокой неопределенности. При несомненных достоинствах и широком признании статистического (вероятностного) подхода применение его ограничено в процессах создания систем защиты информации, оценки и управлении рисками нарушения критически важных свойств защищаемых ресурсов с обозначенными свойствами. В качестве критически важных свойств рассматриваются конфиденциальность, целостность и доступность защищаемых ресурсов с различными категориями важности. Оценка рисков нарушения критически важных свойств непосредственно связана с оценкой эффективности систем защиты информации и выполнена для модели распределения механизмов защиты по нейтрализуемым угрозам. Для каждого уровня защиты определены значения потенциального риска от реализации актуальных угроз. Оценку рисков нарушения критически важных свойств можно применить при проектировании и разработке автоматизированных систем различного назначения, в том числе систем государственного и военного управления.*

Ключевые слова: *конфиденциальность, целостность, доступность, механизмы защиты, неопределенность, уровни защиты, угрозы безопасности, риски, ущерб*

DOI: *10.21681/2311-3456-2019-1-18-24*

Введение

В современном мире требования к автоматизированным системам управления различного назначения значительно изменились: они больше не могут оставаться изолированными от внешнего мира. Возрастающая роль решений в области автоматизации технологических процессов и управления в рамках концепций промышленного интернета вещей (Industrial Internet of Things – IIoT) [1, 2] и распределенного реестра (блокчейн – англ. blockchain) [3, 4] могут существенно упростить и радикально повлиять на эффективность многих технологических и управленческих процессов в автоматизированных системах, повысить рентабельность предприятий социально-экономических отраслей.

В настоящее время осуществляются масштабные изменения в развитии социально-экономических отраслей, характеризующиеся переходом на качественно новый уровень использования информационно-коммуникационных технологий. Появились и активно используются такие понятия как *«Цифровые технологии»* и *«Национальный сегмент цифровой экономики»* [5, 6].

Однако при этом возникают и новые риски для управленческой деятельности, связанные с киберугрозами [7].

Мотивы кибератак многообразны – это получение финансовой выгоды, желание нанести ущерб конкурентам, оказать политическое давление. Порой атаки совершаются по личным мотивам недовольными сотрудниками или подрядчиками. Вне зависимости от мотивов ущерб от несанкционированного вторжения в автоматизированные системы оказывается очень весомым. Это не только внеплановые остановки производства и поломки оборудования, но и серьезные потери в репутации, утечка кон-

1 Братченко Анатолий Иванович, кандидат технических наук, заместитель начальника управления планирования, координации и сопровождения научных исследований АО «Концерн «Системпром», Москва, Россия. E-mail: bratchenko@systemprom.ru

2 Бутусов Игорь Викторович, начальник научно-исследовательского управления АО «Концерн «Системпром», Москва, Россия. E-mail: butusigor@yandex.ru

3 Кобелян Арсен Михайлович, первый заместитель начальника научно-исследовательского управления АО «Концерн «Системпром», Москва, Россия. E-mail: arsen@systemprom.ru

4 Романов Александр Анатольевич, доктор технических наук, главный специалист АО «Концерн «Системпром», Москва, Россия. E-mail: ralexhome@yandex.ru

фиденциальной информации, угроза жизни и здоровью людей, рост риска аварий и даже техногенных катастроф.

Количество кибератак на промышленные сети неуклонно растет. Так по данным US-CERT (United States Computer Emergency Readiness Team – американская компьютерная группа реагирования на чрезвычайные ситуации в киберпространстве) с 2006 по 2012 гг. количество киберинцидентов увеличилось на 782%. В 2014 г. было зарегистрировано 245 случаев кибератак на промышленных объектах, а в 2015 г. – уже 295. При этом очевидно, что многие атаки остались вне поля зрения US-CERT. По данным международной консалтинговой корпорации PricewaterhouseCoopers (PwC), средний ущерб от инцидентов в сфере информационной безопасности в оссии в 2015 г. составил 5,3 млн. $, что на 47 % выше, чем годом ранее.[5]

По данным Федеральной службы безопасности России, ущерб от компьютерных атак за последние несколько лет может достигать 1,5% от мирового валового внутреннего продукта или $1 трлн. И эти показатели имеют тенденции к неуклонному росту.[6]

Не очень высокую эффективность программ обеспечения безопасности информации и систем оценки и управления рисками можно объяснить, на наш взгляд, тем, что существующие модели систем защиты информации (СЗИ) автоматизированных систем различного назначения, а также подходы на базе методов оценки и управления рисками критически важных свойств защищаемых ресурсов в неполной мере отражают специфику СЗИ как сложных организационно-технических систем, поведение которых, как правило, отражает динамику слабоструктурированных процессов, характеризующихся высокой степенью неопределенности вследствие нестационарности, неточности и недостаточности наблюдений, нечеткости и нестабильности тенденций [8, 9]. Защита ресурсов автоматизированных систем рассматривается, в основном, как случайный процесс (показатели уязвимости носят вероятностный характер), поэтому и требования к защите определяются терминами и понятиями теории вероятностей, обоснованными в классической теории систем по аналогии с требованиями к надежности технических систем [10]. В этих моделях и методах используется, главным образом, статистическая трактовка количественных оценок, что при несомненных достоинствах и широком признании статистического подхода ограничивает его применение в процессах создании СЗИ, оценке эффективности СЗИ, оценки и управления рисками нарушения критически важных свойств защищаемых ресурсов с обозначенными свойствами.

Таким образом, особую актуальность приобретает научная задача оценки рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем в условиях высокой неопределенности. Актуальность задачи подтверждается и критериями социальной, политической, экономической, экологической значимости и значимости объектов социально-экономических отраслей для обеспечения обороны страны, безопасности государства и правопорядка [7].

Для повышения степени адекватности применяемых моделей реальным процессам необходим переход от статистической (вероятностной) концепции к концепции создания методологического базиса, но основе методов теории нечетких множеств и математической информатики, которые как нельзя лучше подходят для описания и решения задач с высокой степенью неопределенности (например, [9, 11-14]).

1. Постановка задачи

В автоматизированных системах управления защите от угроз безопасности информации подлежат программно-аппаратные среды, реализуемый на ее основе прикладной функционал (бизнес-процессы), позволяющий накапливать, хранить и обрабатывать сведения, данные и информацию (далее – защищаемые ресурсы) в соответствии с бизнес-процессами системы. Меры и механизмы защиты, реализующие функции защиты в составе СЗИ, предназначены для обеспечения таких критических свойств защищаемых ресурсов с различными категориями важности, как конфиденциальность, целостность и доступность.

Будем рассматривать модель СЗИ с распределением механизмов защиты по нейтрализуемым угрозам безопасности информации, уточняющую более общую модель защиты с полным перекрытием. При построении данной модели в качестве исходной взята естественная посылка, состоящая в том, что в СЗИ должен содержаться по крайней мере один механизм защиты для нейтрализации любой потенциально возможной угрозы безопасности информации.

Представим модель СЗИ в виде кортежа:

$$MOD_{СЗИ} = <\{UR\},\{UG\},\{MZ\},\{KR\},\{TR\},\{ZR\},\{KV\},\{kvk\}>.$$

В рассматриваемой модели

$ur_u \in UR$ – уровни защиты в СЗИ, $u = \overline{1,U}$, U – количество уровней защиты;

$ur_n \in UG$ – множество потенциальных угроз безопасности информации для защищаемых ресурсов, $n = \overline{1,N}$, N – количество актуальных угроз;

$MZ = \{mz_k\} = \bigcup_{u=1}^{U}(MZ_u = \{mz_{k \in K_u, u}\})$ – множество механизмов защиты, где MZ_u – подмножество механизмов защиты уровня защиты $ur_u \in UR$, $k \in K_u$ – подмножество индексов $k = \overline{1,K}$ механизмов защиты на этом уровне, $\bigcup_u K_u = K$, $\bigcap_u K_u = \varnothing$ – механизмы защиты распределены по уровням защиты или, другими словами, каждый механизм защиты принадлежит только одному уровню защиты;

$kr_j \in KR, j = \overline{1,J}$ – множество критериев оценки эффективности механизмы защиты;

$tr_{mz_{ku}} \in TR$ – множество требований к механизмам защиты: $tr_{mz_{ku}} = \{rsk^{\partial on}_{mz_{ku}}, st_{mz_{ku}}, st^{\max}_{mz_{ku}}\}$ где $rsk^{\partial on}_{mz_{ku}}$ – допустимый уровень риска от реализации угрозы, $st_{mz_{ku}}$ – затраты на внедрение механизма за-

5 http://www.idexpert.ru/reviews/13372/

6 https://rns.online/internet/FSB-otsenila-uscherb-ot-kiberatak-v-mire-v-1-trln-2017-02-02/

щиты mz_{ku} в СЗИ, $st_{mz_{ku}}^{\max}$ – максимально допустимые затраты на средства защиты (для класса функционально-однотипных механизмов защиты).

Угрозу ug_n представим в виде вектора $ug_n = \{p^{ug_n}, uch^{ug_n}, rsk^{ug_n} = p^{ug_n} \times uch^{ug_n}\}$[15], где p^{ug_n} – оценка возможности возникновения угрозы ug_n, uch^{ug_n} – ущерб от реализации угрозы ug_n, rsk^{ug_n} – риск от реализации угрозы ug_n, (потенциальные потери)

В модели СЗИ определены множества $zr_z \in ZR$ защищаемых ресурсов автоматизированных систем, $z = \overline{1,Z}$, Z – количество защищаемых ресурсов, и категорий важности $KV = \{kv_v\}, v = \overline{1,V}$ которые могут быть присвоены защищаемым ресурсам в зависимости от их ценности в реализуемых автоматизированной системой бизнес-процессах: $\mu_{KV}(zr_z, kv_v))$ – степень соответствия защищаемого ресурса $zr_z \in ZR$ категории важности kv_v (например, kv_1 - особо важная, kv_2 - очень важная, kv_3 - важная, или kv_4 – мало важная).

Меры и механизмы защиты, реализующие функции защиты, в составе СЗИ предназначены для обеспечения критических свойств $kvk = \{knf, cls, dst\}$ защищаемых ресурсов: knf – конфиденциальность, cls – целостность и dst – доступность.

Потенциальные угрозы безопасности информации $ug_n \in UG$ воздействуют на защищаемые ресурсы $zr_z \in ZR$ с целью нарушения их критических свойств: $UG \times ZR \to GZ$, $\mu_{GZ}(ug_n, zr_z) \to [0,1]$ – оценка возможности воздействия угрозы ug_n на защищаемый ресурс zr_z.

В случае воздействия угрозы ug_n на целостность или доступность защищаемого ресурса zr_z определена оценка возможности восстановления его первоначальных свойств $p_{вст.zr_z}(\tau)$ за заданное время τ.

Понятно, что оценка рисков нарушения критически важных свойств защищаемых ресурсов $rsk_{kvk}^{zr_z \cdot ug_n}$ от реализации угрозы $ug_n \in UG$ непосредственно связана с оценкой эффективности СЗИ $EF_{СЗИ}^{ug_n}$. Исходной посылкой при разработке модели оценки эффективности СЗИ является почти очевидное предположение: с одной стороны, нарушение защищенности ресурсов наносит определенный ущерб, с другой, обеспечение защиты ресурсов сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и ожидаемых потерь от нарушения критически важных свойств защищаемых ресурсов.

Изменяемыми параметрами (в допустимых пределах) при оценке рисков являются время восстановления первоначальных свойств защищаемых ресурсов (при нарушении целостности и доступности) и стоимость СЗИ, поскольку распределение механизмов защиты по нейтрализуемым угрозам безопасности информации теоретически может быть избыточным. Таким образом, появляется возможность управления рисками, а, следовательно, и эффективностью СЗИ.

Формальную постановку задачи представим следующим образом – требуется найти максимум функции эффективности СЗИ при ограничениях на допустимые стоимость СЗИ и время восстановления защищаемых ресурсов $p_{вст.zr_z}(\tau)$:

$$\max EF_{СЗИ}^{ug_n} = \frac{rsk_{kvk}^{ug_n} - (rsk_{kvk}^{zr_z \cdot ug_n} + st_{mz})}{rsk_{kvk}^{ug_n}} \Big| st_{mz} \le st_{СЗИ}^{доп}, \tau \le \tau^{доп},$$

где $RISK_{kvk}^{ug_n} = uch^{ug_n} \times p^{ug_n}$ – потенциальные потери (риск) от реализации угрозы ug_n с целью воздействия на свойства $kvk = \{knf, cls, dst\}$ защищаемых ресурсов, $rsk_{kvk.}^{zr_z \cdot ug_n} = uch^{ug_n} * \mu_{kvk}^{zr_z \cdot ug_n}$ – риск от реализации угрозы $ug_n \in UG$ по отношению защищаемого ресурса zr_z при условиях ее возникновения и не нейтрализации соответствующими механизмами защиты, $st_{mz} = \sum_{u \in U} \sum_{r \in K_u} st_{mz_{r \in K_u, u}}$ – затраты на внедрение механизмов защиты (стоимость СЗИ).

Предлагаемая постановка задачи предполагает, во-первых, знание (или умение определять) ожидаемые потери при нарушении критически важных свойств защищаемых ресурсов, а во-вторых, установление зависимости между уровнем защищенности и средствами, затрачиваемыми на защиту ресурсов. Решение первого вопроса, т.е. оценки ожидаемых потерь при нарушении защищенности ресурсов, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной, коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении критически важных свойств защищаемых ресурсов, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования предлагаемого подхода к оценке рисков. Для определения уровня затрат, обеспечивающих требуемый уровень защищенности ресурсов, необходимо по крайней мере знать, во-первых, полный перечень угроз безопасности информации, во-вторых, потенциальную опасность для защищаемых ресурсов каждой из угроз и, в третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

Поскольку оптимальное решение вопроса о целесообразной величине затрат на защиту заключается в обеспечении равенства этой величины величине ожидаемых потерь $rsk_{kvk}^{zr_z \cdot ug_n} = st_{mz}^{опт}$ при нарушении критически важных свойств защищаемых ресурсов, то достаточно определить только уровень ожидаемых потерь.

2. Ограничения

В научной литературе и стандартах, как правило, рассматривается трехуровневый подход к оценке рисков – уровень автоматизированной системы управления, уровень бизнес-процессов и организационный уровень [16-18]. На уровне системы определяют перечень защищаемых ресурсов, уязвимостей и угроз безопасности информации, а также применяемых мер и механизмов защиты. Этой информации достаточно для оценки возможности возникновения ущерба. Ценность защищаемых ресурсов и соответственно величина ущерба определяется преимущественно на уровне бизнес-процессов и организационном уровне с привлечением владельцев бизнес-процессов, руководства организации/предприятия и прочих заинтересованных лиц. В предлагаемой статье задача оценки величины ущерба от нарушения

критических свойств защищаемых ресурсов не ставится, что позволяет анализировать только уровень автоматизированной системы с соответствующей ему структурой СЗИ. Под ущербом будем понимать вред, потери, урон, наносимые системе и способные привести к невозможности выполнения или ненадлежащему выполнению ею своих функций и/или не достижению целей функционирования системы без дополнительных затрат материальных, трудовых и/или иных видов ресурсов [17, 19].

Значения рисков от потери конфиденциальности, целостности и доступности защищаемых ресурсов будем определять раздельно. Примем также, что угрозы безопасности информации возникают независимо друг от друга и поэтому возникновение одной из них не обязательно приведёт к возникновению других. Реализация угрозы безопасности информации не всегда влечёт за собой нарушение критических свойств защищаемых ресурсов и поэтому для каждой угрозы определяется возможность того, что её реализация приведет к нарушению критически важных свойств защищаемых ресурсов.

Потенциальные угрозы безопасности информации эксплуатируют известные уязвимости в автоматизированных системах управления.

3. Оценка возможностей нейтрализации механизмами защиты потенциальных угроз

Основным результатом применения модели распределения механизмов защиты по нейтрализуемым угрозам безопасности информации (далее – модель распределения) являются подмножества M_n механизмов защиты mz_k, наиболее эффективно нейтрализующих потенциальную ug_n: $M_n = \{mz_k \mid \mu_{\tilde{A}_n}(mz_k, ug_n) \geq pr\}$. Здесь $\tilde{A}_n$ – нечеткое множество предпочтений механизмов защиты при нейтрализации потенциальной угрозы ug_n, $\mu_{\tilde{A}_n}(mz_k, ug_n)$ – функция принадлежности механизма защиты mz_k к нечеткому множеству $\tilde{A}_n$ (интерпретируется как оценка возможности нейтрализации механизмом защиты mz_k потенциальной угрозы ug_n), pr– семантический порог предпочтения функций защиты относительно нейтрализуемых угроз безопасности информации.

Семантический порог предпочтения определяется с учетом частных критериев эффективности, применяемых как к механизмам защиты, так и к нейтрализуемым угрозам: стоимость функций защиты/стоимость нейтрализации актуальной угрозы (критерий kr_1); средневзвешенное количеств угроз, нейтрализуемых механизмом защиты/ средневзвешенное количество механизмов защиты, нейтрализующих актуальную угрозу (критерий kr_2); величина предотвращаемого механизмом защиты риска от реализации актуальных угроз/величина предотвращаемого риска от реализации угрозы (критерий kr_3); степень доверия к механизму защиты/степень доверия к механизму защиты по отношению нейтрализуемых угроз (критерий kr_4); степень совместимости механизмов защиты/степень совместимости механизмов защиты по отношению к нейтрализуемым угрозам (критерий kr_5).

4. Оценка рисков нарушения критически важных свойств

В силу того, что подмножества $M_n = \{mz_k \mid \mu_{\tilde{A}_n}(mz_k, ug_n) \geq pr\}$ могут включать в себя больше одного механизмов защиты mz_k (избыточность механизмов защиты mz_k при нейтрализации угрозы ug_n), то для нейтрализации угрозы ug_n теоретически предпочтительными могут оказаться несколько механизмов защиты $mz_k \in M_n$ как по уровням СЗИ, так и на уровне СЗИ автоматизированной систем в целом.

Для модели распределения определено нечеткое множество $\tilde{MG} = \{\mu_{\tilde{A}_n}(mz_k, ug_n)\} = \{\mu_{\tilde{MG}}(mz_k, ug_n)\}$, $k = \overline{1, K}$, $n = \overline{1, N}$ представляющее собой матрицу размера $K \times N$ [20].

По уровням защиты $ur_u \in UR$ в СЗИ, $u = \overline{1, U}$, механизмы защиты представлены подмножествами $M_{ru} = \{mz_{k \in K_u, u} \mid \mu_{\tilde{A}_n}(mz_{k \in K_u, u}, ug_n) \geq pr\}$, $k \in K_u$ – индексы механизмов защиты, задействованных на уровне защиты $ur_u \in UR$ для нейтрализации угрозы ug_n. Тогда $\mu^{ug_{ru}} = p^{ug_n} \times \prod_{K_u} \{1 - \mu_{\tilde{A}_n}(mz_{k \in K_u, u}, ug_n)\}$ представляет собой оценку возможности реализации угрозы на уровне защиты ur_u с учетом возможности ее возникновения и при условии, что p^{ug_n} ее не смогли нейтрализовать соответствующие механизмы защиты: $\prod_{K_u} \{1 - \mu_{\tilde{A}_n}(mz_{k \in K_u, u}, ug_n)\}$ – вероятностное пересечение нечетких множеств. При степени воздействии $\mu_{GZ}(ug_n, zr_z)$ угрозы ug_n на защищаемый ресурс zr_z с категорией важности $\mu_{KV}(zr_z, kv_v)$ оценку возможности нарушения конфиденциальности можно вычислить по формуле $\mu_{cnf.u}^{zr_z.ug_n} = (1 - (1 - \mu^{ug_{ru}} \times \mu_{KV}(zr_z, kv_v) \times \mu_{GZ}(ug_n, zr_z)))$, а потенциальные потери или риск от нарушения конфиденциальности по формуле $rsk_{cnf.u}^{zr_z.ug_n} = uch^{ug_n} * \mu_{cnf.u}^{zr_z.ug_n}$.

Оценку возможности нарушения конфиденциальности защищаемого ресурса zr_z в СЗИ в целом выполним с помощью следующего выражения: $\mu_{cnf}^{zr_z.ug_n} = (1 - (1 - \mu^{ug_{ru}} \times \mu_{KV}(zr_z, kv_v) \times \mu_{GZ}(ug_n, zr_z) \times \prod_{u \in U} \mu^{ug_{ru}}))$. Соответственно потенциальные потери или риск от нарушения конфиденциальности защищаемого ресурса zr_z от воздействия угрозы ug_n определи как $rsk_{cnf}^{zr_z.ug_n} = uch^{ug_n} * \mu_{cnf}^{zr_z.ug_n}$.

В случае воздействия угрозы ug_n на целостность или доступность защищаемого ресурса zr_z предусматривается процедура восстановления его первоначальных свойств в виде оценки возможности $p_{вст.zr_z}(\tau)$ восстановления за время τ. С учетом этой оценки и ранее полученных результатов приведем выражения для оценки нарушения свойств целостности и доступности защищаемых ресурсов с различными категориями важности.

1. Нарушение целостности.

1.1. По уровням СЗИ.

1.1.1. Оценка возможности нарушения целостности: $\mu_{cls.u}^{zr_z.ug_n} = (1 - (1 - \mu^{ug_{ru}} \times \mu_{KV}(zr_z, kv_v) \times \mu_{GZ}(ug_n, zr_z) \times (1 - p_{вст.zr_z}^{cls}(\tau))))$.

1.1.2. Потенциальные потери или риск от нарушения целостности: $rsk_{cls.u}^{zr_z.ug_n} = uch^{ug_n} \times \mu_{cls.u}^{zr_z.ug_n}$.

1.2. На уровне СЗИ в целом.

1.2.1. Оценка возможности нарушения целостности: $\mu_{cls}^{zr_z.ug_n} = (1 - (1 - \mu^{ug_{ru}} \times \mu_{KV}(zr_z, kv_v) \times \mu_{GZ}(ug_n, zr_z) \times (1 - p_{вст.zr_z}^{cls}(t)) \times \prod_{ue U} \mu^{ug_{ru}}))$.

1.2.2. Потенциальные потери или риск от нарушения целостности: $rsk_{cls}^{zr_z.ug_n} = uch^{ug_n} \times \mu_{cls}^{zr_z.ug_n}$.

2. Нарушение доступности.

2.1. По уровням СЗИ.

2.1.1. Оценка возможности нарушения доступности: $\mu_{dst.u}^{zr_z.ug_n} = (1-(1-\mu^{ug_{nu}} \times \mu_{KV}(zr_z, kv_v) \times \mu_{GZ}(ug_n, zr_z) \times (1-p_{вст.zr_z}^{dst}(t))))$.

2.1.2. Потенциальные потери или риск от нарушения доступности: $rsk_{dst.u}^{zr_z.ug_n} = uch^{ug_n} \times \mu_{dst.u}^{zr_z.ug_n}$.

2.2. На уровне СЗИ в целом.

2.2.1. Оценка возможности нарушения доступности: $\mu_{dst}^{zr_z.ug_n} = (1-(1-\mu^{ug_{nu}} \times \mu_{KV}(zr_z, kv_v) \times \mu_{GZ}(ug_n, zr_z) \times (1-p_{вст.zr_z}^{dst}(t)) \times \prod_{u \in U} \mu^{ug_{nu}}))$.

2.2.2. Потенциальные потери или риск от нарушения доступности: $rsk_{dst}^{zr_z.ug_n} = uch^{ug_n} \times \mu_{dst}^{zr_z.ug_n}$

Представленные оценки рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления предполагают избыточность механизмов защиты как по уровням СЗИ, так и в структуре СЗИ в целом. Мы рассматриваем эффективность СЗИ как функцию

$$EF_{СЗИ} = \frac{rsk_{kvk}^{ug_n} - (rsk_{kvk}^{zr_z.ug_n} + st_{mz})}{rsk_{kvk}^{ug_n}},$$

где $rsk_{kvk}^{ug_n} = uch^{ug_n} \times p^{ug_n}$ – риск от реализации угрозы с целью воздействия на критически важные свойства $kvk = \{knf, cls, dst\}$ защищаемых ресурсов, $rsk_{kvk.}^{zr_z.ug_n} = uch^{ug_n} \times \mu_{kvk}^{zr_z.ug_n}$ – риск от реализации угрозы по отношению защищаемого ресурса zr_z при условиях ее возникновения и не нейтрализации соответствующими механизмами защиты, $st_{mz} = \sum_{u \in U} \sum_{r \in K_u} st_{mz_{r \in K_u, u}}$ – затраты на внедрение механизмов защиты, то имеется возможность ее оптимизации путем подбора механизмов защиты по затратам на внедрение как по уровням СЗИ, так и в структуре СЗИ в целом (устранение избыточности механизмов защиты, что приведет к снижению оценок возможности нейтрализации соответствующих угроз безопасности информации), а также выбором времени восстановления целостности и доступности защищаемых ресурсов.

Выражение $d_{kvk}^{ug_n} = \frac{\max_{zr_z} rsk_{kvk}^{zr_z.ug_n}}{rsk_{kvk}^{ug_n}}$ определяет коэффициент опасности угрозы ug_n в плане воздействия на критически важное свойство $kvk = \{knf, cls, dst\}$ защищаемых ресурсов $zr_z \in ZR$.

Риск от нарушения свойства kvk в автоматизированной системе оценивается как $rsk_{kvk} = \max_{zr_z} \max_{ug_n} rsk_{kvk}^{zr_z.ug_n}$, а оценка полного риска нарушения свойств конфиденциальности, целостности и доступности как $rsk = \max\{rsk_{knf}, rsk_{cls}, rsk_{dst}\}$.

Выводы

1. Обоснована теоретическая и практическая актуальность научной задачи оценки в условиях высокой неопределенности рисков нарушения критически важных свойств защищаемых ресурсов – конфиденциальности, целостности и доступности защищаемых ресурсов с различными категориями важности.

2. В известных моделях формирования структуры СЗИ и методах оценки рисков нарушения критически важных свойств, главным образом, используется статистическая трактовка количественных оценок в терминах теории вероятностей, что при несомненных достоинствах и широком признании статистического подхода затрудняет решение задачи оценки рисков в условиях высокой неопределенности.

3. Приведена постановка и решена научная задача оценки в условиях высокой неопределенности рисков нарушения критически важных свойств защищаемых ресурсов – конфиденциальности, целостности и доступности защищаемых ресурсов с различными категориями важности. Оценка рисков непосредственно связана с оценкой эффективности систем защиты информации в составе автоматизированных систем. Определены ограниче6ния и допущения для решения поставленной задачи.

4. Адекватность оценок рисков нарушения критически важных свойств защищаемых ресурсов существенным образом зависит от выбранной модели СЗИ. Наиболее эффективной для оценок рисков является модель распределения механизмов защиты по нейтрализуемым угрозам безопасности информации.

5. Оценка рисков нарушения критически важных свойств может быть применена при проектировании и разработке автоматизированных систем управления различного назначения, защищаемые ресурсы которых имеют различные категории важности.

Литература:

1. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 2 (26). С. 2-15.
2. Петренко С.А., Петренко А.С. Инновационные технологии интернета вещей // Защита информации. Инсайд. 2017. № 6 (78). С. 22-30.
3. Захаров Д.Н., Иванов В.Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. 2017. № S2 (20). С. 30-38.
4. Кустов В.Н., Станкевич Т.Л. Еще раз о технологии Blockchain // Защита информации. Инсайд. 2018. № 2 (80). С. 68-74.
5. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 1 // Вопросы кибербезопасности. 2014. № 1 (2). С. 61-66.
6. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. - River Publishers, 2018. 458 p.
7. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

8. Бутусов И.В., Нащекин П.А., Романов А.А. Теоретико-семантические аспекты организации комплексной системы защиты информационных систем // Вопросы кибербезопасности. 2016. №1 (14). С. 9-16.
9. Щербаков Е.С., Корчагин П.В. Применение методов теории возможностей при моделировании систем защиты информации // Вопросы кибербезопасности. 2017. №1(19). С. 2-5. DOI: 10.21681/2311-3456-2017-1-2-5.
10. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. Под ред. А.С. Маркова. М., Радио и связь, 2012. 192 с.
11. Бурлак Д.Ю., Седаков А.В., Сударенко А.Н., Соколов П.С. Математическая модель оценки эффективности функционирования системы защиты АСУ от непреднамеренной выдачи распорядительной информации // Известия Института инженерной физики. 2010. № 2 (16). С. 44-46.
12. Данилюк С.Г., Мурашко А.А. Применение вероятностно-лингвистического подхода при решении задачи оценки уязвимости системы обеспечения безопасности эксплуатации важных технических объектов // Известия Института инженерной физики. 2016. № 2 (40). С. 5-12.
13. Захаренков А.И., Бутусов И.В., Романов А.А. Степень доверенности программно-аппаратных средств как показатель качества замещения импорта // Вопросы кибербезопасности. 2017. № 4 (22). С. 2-9.
14. Стародубцев П.Е., Соколовский Е.П., Бухаров Е.О. Управление запасами ключей криптографического обмена на основе алгоритма нечеткого логического вывода Сугено // Известия Института инженерной физики. 2018. № 3 (49). С. 94-96.
15. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. №1 (14). С. 17-23
16. Бибашов С.А. Модель формирования требований по защите информации к создаваемым автоматизированным системам в защищенном исполнении // Вопросы кибербезопасности. 2017. №5 (24). С. 83-90.
17. Нурдинов Р.А. Определение вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей // Современные проблемы науки и образования. 2014. № 3. URL: http://science-education.ru/ru/article/view?id=13290.
18. Яндыбаева Э.Э., Машкина И.В. Разработка модели планирования используемых средств защиты информации для информационных систем электронных торговых площадок // Вестник Уфимского государственного авиационного технического университета. 2015. Т. 19. № 1. С. 264-269.
19. Чабонян В.А., Шахалов Ю.И. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1 (1). С. 17-27.
20. Мурзин А.П., Бутусов И.В., Романов А.А. Адаптация системы защиты информации автоматизированных систем управления к нейтрализуемым угрозам // Приборы и системы. Управление, контроль, диагностика. Автоматизированные системы управления. 2017. №10. С. 1–7.

Рецензент: *Стародубцев Юрий Иванович, заслуженный деятель науки Российской Федерации, доктор военных наук, профессор 32 кафедры Военной академии связи им. С.М. Буденного, г. Санкт-Петербург, Россия. E-mail : malika.davliatova@gmail.com*

APPLICATION OF METHODS OF THEORY OF FUZZY SETS TO ASSESS THE RISK OF VIOLATIONS OF CRITICAL PROPERTIES PROTECTED RESOURCES AUTOMATED CONTROL SYSTEM

Bratchenko A.I.[7], Butusov I.V.[8], Kobalyan A.M.[9], Romanov A.A.[10]

The purpose of the article is to increase the reliability of risk assessments of violations of critical properties of protected resources with different categories of importance in conditions of high uncertainty.

Method: *modeling the distribution of protection mechanisms for neutralized threats to information security and the use of fuzzy theory methods to assess the risks of violations of critical properties.*

The result: *it is shown that the existing models of information security systems and methods of risk assessment of violations of critical properties of protected resources do not fully reflect the specifics of information security systems as complex organizational and technical systems. The behavior of such systems reflects the dynamics of semi-structured processes characterized by a high degree of uncertainty due to unsteadiness, inaccuracy and insufficiency of observations, fuzzy and unstable trends. The urgency of the scientific problem of risk assessment of violation of critical properties of protected resources in conditions of high uncertainty is substantiated. With the undoubted*

7 Anatoly I. Bratchenko, candidate of technical Sciences, Deputy head of personnel training and support of scientific research of JSC «Concern « Sistemprom», Moscow, Russia. E-mail: bratchenko@systemprom.ru
8 Igor V. Butusov, Head of Research Department JSC “concern SYSTEMPROM”, Moscow, Russia. E-mail: butusigor@yandex.ru
9 Arsen M. kobalyan, first Deputy head of the research Department of JSC «Concern «Sistemprom», Moscow, Russia. E-mail: arsen@systemprom.ru
10 Aleksandr A. Romanov, Doctor of Technical Sciences, Chief specialist JSC “concern SYSTEMPROM”, Moscow, Russia. E-mail: ralexhome@yandex.ru

advantages and wide recognition of the statistical (probabilistic) approach, its application is limited in the processes of creating information security systems, assessment and risk management of violations of critical properties of protected resources with designated properties. Confidentiality, integrity and availability of protected resources with different categories of importance are considered as critical properties. The risk assessment of violation of critical properties is directly related to the assessment of the effectiveness of information security systems and is performed for the model of distribution of protection mechanisms for neutralizable threats. For each level of protection, the values of the potential risk from the implementation of actual threats are determined. Risk assessment of critical properties violations can be applied in the design and development of automated systems for various purposes, including systems of state and military administration.

Keywords: *confidentiality, integrity, availability, mechanisms of protection, uncertainty, levels of protection, security threats, risks, damage*

References:

1. Zegzhda D.P., Vasil'ev YU.S., Poltavceva M.A., Kefeli I.F., Borovkov A.I. Kiberbezopasnost' progressivnyh proizvodstvennyh tekhnologij v ehpohu cifrovoj transformacii // Voprosy kiberbezopasnosti. 2018. № 2 (26). S. 2-15.
2. Petrenko S.A., Petrenko A.S. Innovacionnye tekhnologii interneta veshchej // Zashchita informacii. Insajd. 2017. № 6 (78). S. 22-30.
3. Zaharov D.N., Ivanov V.YU. Bezopasnost' v sfere oborota virtual'noj valyuty // Voprosy kiberbezopasnosti. 2017. № S2 (20). S. 30-38.
4. Kustov V.N., Stankevich T.L. Eshche raz o tekhnologii Blockchain // Zashchita informacii. Insajd. 2018. № 2 (80). S. 68-74.
5. Karckhiya A.A. Kiberbezopasnost' i intellektual'naya sobstvennost'. CHast' 1 // Voprosy kiberbezopasnosti. 2014. № 1 (2). S. 61-66.
6. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. - River Publishers, 2018. 458 p.
7. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
8. Butusov I.V., Nashchekin P.A., Romanov A.A. Teoretiko-semanticheskie aspekty organizacii kompleksnoj sistemy zashchity informacionnyh sistem // Voprosy kiberbezopasnosti. 2016. №1 (14). S. 9-16.
9. SHCHerbakov E.S., Korchagin P.V. Primenenie metodov teorii vozmozhnostej pri modelirovanii sistem zashchity informacii // Voprosy kiberbezopasnosti. 2017. №1(19). S. 2-5. DOI: 10.21681/2311-3456-2017-1-2-5.
10. Markov A.S., Cirlov V.L., Barabanov A.V. Metody ocenki nesootvetstviya sredstv zashchity informacii. Pod red. A.S. Markova. M., Radio i svyaz', 2012. 192 s.
11. Burlak D.YU., Sedakov A.V., Sudarenko A.N., Sokolov P.S. Matematicheskaya model' ocenki ehffektivnosti funkcionirovaniya sistemy zashchity ASU ot neprednamerennoj vydachi rasporyaditel'noj informacii // Izvestiya Instituta inzhenernoj fiziki. 2010. № 2 (16). S. 44-46.
12. Danilyuk S.G., Murashko A.A. Primenenie veroyatnostno-lingvisticheskogo podhoda pri reshenii zadachi ocenki uyazvimosti sistemy obespecheniya bezopasnosti ehkspluatacii vazhnyh tekhnicheskih ob»ektov // Izvestiya Instituta inzhenernoj fiziki. 2016. № 2 (40). S. 5-12.
13. Zaharenkov A.I., Butusov I.V., Romanov A.A. Stepen' doverennosti programmno-apparatnyh sredstv kak pokazatel' kachestva zameshcheniya importa // Voprosy kiberbezopasnosti. 2017. № 4 (22). S. 2-9.
14. Starodubcev P.E., Sokolovskij E.P., Buharov E.O. Upravlenie zapasami klyuchej kriptograficheskogo obmena na osnove algoritma nechetkogo logicheskogo vyvoda Sugeno // Izvestiya Instituta inzhenernoj fiziki. 2018. № 3 (49). S. 94-96.
15. Olad'ko V.S. Model' vybora racional'nogo sostava sredstv zashchity v sisteme ehlektronnoj kommercii // Voprosy kiberbezopasnosti. 2016. №1 (14). S. 17-23
16. Bibashov S.A. Model' formirovaniya trebovanij po zashchite informacii k sozdavaemym avtomatizirovannym sistemam v zashchishchennom ispolnenii // Voprosy kiberbezopasnosti. 2017. №5 (24). S. 83-90.
17. Nurdinov R.A. Opredelenie veroyatnosti narusheniya kriticheskih svojstv informacionnogo aktiva na osnove CVSS metrik uyazvimostej // Sovremennye problemy nauki i obrazovaniya. 2014. № 3. URL: http://science-education.ru/ru/article/view?id=13290.
18. YAndybaeva EH.EH., Mashkina I.V. Razrabotka modeli planirovaniya ispol'zuemyh sredstv zashchity informacii dlya informacionnyh sistem ehlektronnyh torgovyh ploshchadok // Vestnik Ufimskogo gosudarstvennogo aviacionnogo tekhnicheskogo universiteta. 2015. T. 19. № 1. S. 264-269.
19. CHabonyan V.A., SHalahov YU.I. Analiz i sintez trebovanij k sistemam bezopasnosti ob»ektov kriticheskoj informacionnoj infrastruktury // Voprosy kiberbezopasnosti. 2013. № 1 (1). S. 17-27.
20. Murzin A.P., Butusov I.V., Romanov A.A. Adaptaciya sistemy zashchity informacii avtomatizirovannyh sistem upravleniya k nejtralizuemym ugrozam // Pribory i sistemy. Upravlenie, kontrol', diagnostika. Avtomatizirovannye sistemy upravleniya. 2017. №10. S. 1–7.