УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 54–61

Собина А.А., Лизовенко О.А., Пономарева О.А., Чернова О.В.

DOI: 10.14529/secur220306

ПОДХОДЫ К ОЦЕНКЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОФИЦИАЛЬНОГО ВЕБ-САЙТА ОРГАНИЗАЦИИ

В статье представлены подходы к оценке угроз безопасности информации в том случае, когда владелец информационного ресурса обладает правом самостоятельно выбирать способ такой оценки. Официальный веб-сайт коммерческой организации, представленный в статье, не относится к информационным системам, для которых нормативно установлен порядок оценки угроз безопасности информации, в том числе: информационным системам персональных данных, государственным (муниципальным) информационным системам и пр. Для подготовки статьи были изучены соответствующие нормативные правовые акты и методические документы федеральных органов исполнительной власти Российской Федерации, международные стандарты. В качестве основы взяты методический документ «Методика оценки угроз безопасности информации» (05.02.2021 г.) и стандарт ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». В процессе подготовки статьи авторами разработаны наглядные схемы, отражающие основные этапы оценки угроз безопасности информации (оценки рисков). Указанные этапы реализованы для рассматриваемой информационной системы.

Ключевые слова: *угрозы безопасности информации, модель угроз безопасности информации, оценка угроз, ИСО, веб-сайт.*

Sobina A.A., Lizovenko O.A., Ponomareva O.A., Chernova O.V.

APPROACHES TO INFORMATION SECURITY THREATS ASSESSMENT FOR THE OFFICIAL WEBSITE OF THE ORGANIZATION

The article provides approaches to the information security threats assessment in the case when the owner of an information resource has the right to choose an approach to the assessment. The official website of the organization presented in the article is not an information system that implies a strict approach to information security threats assessment because the information system does not process personal data, state information resources and other similar data. To prepare the article, regulatory and methodological documents of the federal

executive authorities of the Russian Federation, international standards were studied. As the basis, methodological document «Methodology for assessing threats to information security» (February 5, 2021) and standard ISO/IEC 27005 «Information technology. Security techniques. Information Security Risk Management» were taken. The authors have prepared schemes with the main stages of information security threat assessment (risk assessment). Each described stage is implemented for the considered information system.

Keywords: *information security threats, information security threat model, threats assessment, ISO, website.*

1. Введение

Одним из важнейших этапов создания системы защиты информации (защищенной информационной системы) является определение угроз безопасности информации (далее – УБИ), реализация которых может привести к нарушению безопасности информации (оценка угроз), и разработка на их основе модели угроз безопасности информации.

Корректно разработанная модель угроз безопасности информации информационной системы (далее – модель угроз) позволит выбрать оптимальные технические и организационные меры защиты информации и создать эффективную систему защиты информации [1]. Организационные и технические меры должны блокировать (нейтрализовать) актуальные УБИ, представленные в модели угроз.

В случае недостаточности выбранных мер реализация УБИ может привести к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора информационной системы, а в случае обработки персональных данных – для субъектов персональных данных.

Кроме того, обязанность оператора информационной системы (либо владельца информации, заказчика, заключившего контракт на создание информационной системы) определять (оценивать) УБИ предусмотрена нормативными правовыми актами Российской Федерации. Нормативные правовые акты, регламентирующие оценку УБИ, разрабатываются федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

В рамках настоящей статьи не будут рассмотрены аспекты оценки УБИ:

– связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации;

– связанных с техническими каналами утечки информации;

– в финансовой сфере (для финансовых организаций).

2. Подход к оценке угроз безопасности информации в соответствии с требованиями регулятора

Для определения УБИ, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, а также для некоторых других категорий информационных систем, должен использоваться методический документ «Методика оценки угроз безопасности информации», утвержденный 05.02.2021 г. (далее – Методика оценки, методический документ).

Этапы оценки УБИ, представленные в методическом документе, приведены на рис. 1.

Методическим документом определены форма, порядок разработки и актуализации модели угроз.

3. Иностранные (международные) подходы к оценке угроз безопасности информации

Для эффективного управления рисками информационной безопасности разработаны специальные методики, представленные, например, в международных стандартах ISO 15408, ISO 17799 (BS7799), ISO 27000, BSI; а также национальных стандартах NIST 800-'30, SAC, COSO, SAS 55/78 и др. [2].

Как правило, в зарубежных (международных) стандартах и методиках оценка УБИ является составной частью оценки рисков информационной безопасности. Риск информационной безопасности – это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

В рамках настоящей статьи рассматривается стандарт ГОСТ Р ИСО/МЭК 27005–2010 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Менеджмент риска информационной безопасности» (далее –

ИСО/МЭК 27005), так как он переведен на русский язык, утвержден Федеральным агентством по техническому регулированию и метрологии и введен в действие в качестве национального стандарта Российской Федерации.

ИСО/МЭК 27005 представляет руководство по управлению рисками информационной безопасности (далее – ИБ) и предназначен для помощи в реализации процессов информационной безопасности на основе подхода, связанного с менеджментом риска.

Примеры использования ИСО/МЭК 27005 представлены, например, в [3], [4], [5], [6].

Отдельные этапы оценки риска ИБ, представленные в ИСО/МЭК 27005, приведены на рисунке 2.

Оцененные риски ИБ требуют обработки: снижения, сохранения, предотвращения, переноса риска. Если уровень риска соответствует критериям принятия риска, то отсутствует необходимость в реализации дополнительных мер, и риск может быть сохранен (принят).

Таким образом, если проводить параллель с Методикой оценки, соотношение уровня риска ИБ критериям принятия риска – индикатор актуальности (неактуальности) УБИ, соответствующей данному риску.

4. Пример практического применения подходов к оценке угроз безопасности информации

4.1. Исходные данные для оценки

Подходы к оценке угроз (рисков) рассмотрены на примере информационной системы, представляющей собой официальный сайт коммерческой организации (далее – ИС). Указанная организация обладает правом выбора подхода к оценке УБИ, так на рассматриваемый веб-сайт не распространяются требования регулятора.

Сайт размещен на сервере организации и поддерживается ее сотрудниками, а его содержание представляет собой исключительно справочную информацию (каталог услуг, новости, информация о партнерах и клиентах, контакты, вакансии). Кроме того, на сайте нет платежного механизма, формы обратной связи и личного кабинета для клиентов.

4.2. Методика оценки

Этапы оценки УБИ приведены на рисунке 1.

Рис. 1

Рис. 2

В качестве негативных последствий реализации (возникновения) УБИ можно обозначить:

– размещение недостоверной информации на веб-ресурсе организации;

– использование веб-ресурса с целью распространения и управления вредоносным программным обеспечением;

– нарушение функционирования веб-ресурса;

– нарушение деловой репутации.

Объекты воздействия УБИ:

– информация (обрабатываемая в ИС, учетные данные);

– автоматизированное рабочее место администратора сайта;

– сервер;

– системное программное обеспечение;

– прикладное программное обеспечение (обеспечивающее функционирование сайта, веб-браузер);

– телекоммуникационное оборудование;

– обеспечивающие системы (электропитание, кондиционирование);

– каналы связи;

– пользователь (администратор сайта).

Нарушители признаются актуальными, если возможные цели реализации ими УБИ могут привести к определенным для ИС негативным последствиям и соответствующим рискам (видам ущерба). Таким образом, для рассматриваемой ИС актуальными являются следующие виды нарушителей:

– отдельные физические лица (хакеры);

– конкурирующие организации;

– администратор информационной системы;

– бывшие (уволенные) работники (пользователи).

Были учтены следующие цели реализации УБИ, которые могут привести к негативным последствиям:

– получение конкурентных преимуществ;

– любопытство или желание самореализации (подтверждение статуса);

– непреднамеренные, неосторожные или неквалифицированные действия;

– месть за ранее совершенные действия.

Способы реализации УБИ:

– атака типа «отказ в обслуживании»;

– использование уязвимостей прикладного программного обеспечения, используемого для обработки данных;

– действия пользователей (ошибочные или целенаправленные), приводящие к деструктивным последствиям;

– повреждение (вывод из строя) технических средств.

УБИ возможна, если для нее имеются нарушитель, объект воздействия, способ реализации, и ее реализация может привести к негативным последствиям. Перечень возможных угроз формируется из общего перечня УБИ, приведенного в Банке данных угроз (https://bdu.fstec.ru/), путем исключения УБИ, не удовлетворяющих данному условию (например, для исключаемой угрозы УБИ.110 объект воздействия – ресурсные центры грид-системы, которых в ИС нет).

Для каждой из возможных УБИ определяются сценарии реализации на основании представленных в Методике оценки техник и тактик. Чтобы определить все возможные сценарии атак, техники и тактики, получить дополнительную информацию о возможных уязвимостях, способах реализации компьютерных атак могут использоваться Банк данных угроз (https://bdu.fstec.ru/) и другие источники [7].

Например, рассмотрим УБИ.100 «Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб», которая реализуется следующим сценарием: тактика Т1, техника Т1.4 (направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств). Таким образом, данная УБИ должна быть признана актуальной и включена в модель угроз рассматриваемой ИС.

4.3. ИСО/МЭК 27005

Основные этапы оценки риска ИБ приведены на рисунке 2.

До процедуры оценки риска ИБ должны быть определены основные критерии, сфера действия и границы, структура процесса менеджмента риска ИБ.

На первом этапе оценки риска ИБ определяются активы. Активы в ИСО/МЭК 27005 понимаются шире, чем объекты воздействия в Методике оценки.

Основные и вспомогательные активы в рамках ИС, их ценность (по десятибалльной шкале) приведены в таблице 1.

В качестве перечня угроз и их источников принят полный набор данных из приложения С к ИСО/МЭК 27005, за исключением угроз и источников угроз, указанных в таблице 2.

Далее необходимо установить, какие организационные и технические меры реализованы ранее. В организации реализованы следующие меры:

Таблица 1

Активы

Наименование актива	Владелец	Значимость
Бизнес-процесс – размещения информации на официальном сайте с целью обеспечения информационной открытости организации	Руководитель организации	8
Информация	Руководитель организации	6
Автоматизированное рабочее место администратора сайта	Администратор сайта	5
Сервер	Руководитель отдела ИТ	7
Системное программное обеспечение	Администратор сайта	5
Прикладное программное обеспечение	Администратор сайта	5
Телекоммуникационное оборудование	Руководитель отдела ИТ	4
Обеспечивающие системы (электропитание, кондиционирование)	Руководитель отдела ИТ	6
Каналы связи	Руководитель отдела ИТ	4
Пользователь (администратор сайта)	Руководитель организации	4
Помещение серверной и кабинет отдела информационных технологий	Руководитель отдела ИТ	3

Таблица 2

Исключаемые угрозы и их источники

Исключаемая угроза/источник угрозы	Обоснование
Класс угроз, связанных с природными явлениями	Вулканическая и сейсмическая активность в регионе отсутствуют. Помещения расположены на 9 этаже из 14
Перехват компрометирующих сигналов помех	Помехи не используются
Прослушивание	Акустическая информация не обрабатывается
Кража носителей или документов	Защищаемая информация не хранится на отдельных (не встроенных) носителях и в бумажном виде
Поиск повторно используемых или забракованных носителей	Защищаемая информация не хранится на отдельных (не встроенных) носителях и в бумажном виде
Данные из ненадежных источников	Не обрабатывается информация, влияющая на принятие решений
Определение местонахождения	Местонахождение не является конфиденциальной информацией
Террорист	Не соответствует мотивация
Промышленный шпионаж	Не соответствует мотивация

– доступ в крыло на этаже, которое занимает организация, ограничен: установлена металлическая дверь с магнитным замком;

– внедрена система видеонаблюдения;

– внедрена система охранно-пожарной сигнализации с выводом на пункт охраны;

– все помещения оборудованы запираемыми дверьми;

– должностные инструкции сотрудников включают положения по обеспечению ИБ, сотрудники проходят периодическое обучение;

– используются средства антивирусной защиты на всех рабочих станциях;

– используется межсетевой экран на границе с сетью общего доступа;

– серверный сегмент выделен в отдельную виртуальную локальную сеть (VLAN).

Технические уязвимости могут быть определены с использованием автоматизированных инструментальных средств поиска уязвимостей, тестирования и оценки, тестирования на проникновение, проверки кода.

Среди уязвимостей для организации также характерны:

– плохой менеджмент паролей;

– отсутствие резервных копий;

– единая точка отказа;

– отсутствие формального процесса для пересмотра прав пользователей.

Негативные последствия для реализации определяются в виде перечней сценариев инцидентов. Сценарий инцидента – это описание угрозы, использующей определенную уязвимость или совокупность уязвимостей в инциденте ИБ.

Таким образом, для организации, учитывая исходные данные, можно привести следующие сценарии:

a) угроза фальсификации прав, использующая уязвимости, связанные с плохим менеджментом паролей, отсутствием формального процесса для пересмотра прав пользователей, может привести к размещению недостоверной информации на веб-ресурсе организации;

b) угроза отказа телекоммуникационного оборудования, использующая уязвимость, связанную с единой точкой отказа, может привести к нарушению функционирования веб-ресурса;

c) угроза тайных действий с программными средствами, использующая уязвимость, связанную с отсутствием резервных копий, может привести к использованию веб-ресурса с целью распространения и управления вредоносным программным обеспечением.

Оценка последствий осуществляется с учетом ценности активов, которые оказываются затронуты инцидентом. Результаты оценки приведены в таблице 3.

Установление значений уровней рисков производится для всех значимых сценариев инцидентов. В стандарте приведены примеры различных методов и подходов к установлению значений рисков ИБ.

В организации используется подход, приведенный в таблице 4.

Перечень рассмотренных рисков с уровнями присвоенных значений и назначенными приоритетами приведен в таблице 5.

В зависимости от принятых в организа-

Таблица 3

Сравнение сценариев

Сценарий	Ценность	Вероятность
a)	12	Низкая
b)	15	Высокая
c)	8	Средняя

Таблица 4

Критерии оценки

Уровень риска		Вероятность реализации		
		Низкая	Средняя	Высокая
Ценность	1-4	1	3	6
	5-9	2	4	7
	10-14	3	5	8
	15-19	4	6	9
	20+	5	7	10

Таблица 5

Рассмотренные риски

Сценарий	Уровень риска	Ранжирование угроз
a)	3	3
b)	9	1
c)	4	2

ции критериев принятия риска, риск ИБ может быть сохранен (принят) либо потребовать дальнейшей обработки. Предположим, что в организации приемлемый уровень риска – 3.

Таким образом, требуют дальнейшей обработки риски ИБ, описанные сценариями b) и c). В сценариях реализации отражены соответствующие УБИ. Должны быть выбраны меры и средства контроля и управления для снижения, предотвращения или переноса указанных рисков.

5. Заключение

Авторами проанализированы подходы к оценке УБИ и рисков информационной безопасности, изложенные в документах:

– методический документ «Методика оценки угроз безопасности информации», утвержденный 05.02.2021 г.;

– ГОСТ Р ИСО/МЭК 27005–2010 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Менеджмент риска информационной безопасности».

Объем данной статьи не позволяет отразить все практические аспекты оценки УБИ и рисков информационной безопасности или провести более детальное сравнение приведенных выше документов. Поэтому данные вопросы будут рассмотрены в последующих работах.

Литература / References

1. O. Kalugina, I. Barankova and U. Mikhailova, «Development of a Tool for Modeling Security Threats of an Enterprise Information System», 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, P. 1–5, DOI: 10.1109/ICECCE49384.2020.9179449.

2. S. S. Sokolov, O. M. Alimov, M. G. Golubeva, V. G. Burlov and N. M. Vikhrov, «The automating process of information security management», 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, P. 124–127, DOI: 10.1109/EIConRus.2018.8317045.

3. M. M. Putra and K. Mutijarsa, «Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005», 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2021, P. 14–19, DOI: 10.1109/EIConCIT50028.2021.9431865.

4. S. Jaya Putra, M. Nur Gunawan, A. Falach Sobri, J. Muslimin, Amilin and D. Saepudin, «Information

Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company», 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, P. 1–5, doi: 10.1109/CITSM50537.2020.9268845.

5. S. Prasetyo and Y. G. Sucahyo, «Information security risk management planning: A case study at application module of state asset directorate general of state asset ministry of finance», 2014 International Conference on Advanced Computer Science and Information System, 2014, P. 96–101, doi: 10.1109/ICACSIS.2014.7065875.

6. A. Alwi and K. A. Zainol Ariffin, «Information Security Risk Assessment for the Malaysian Aeronautical Information Management System», 2018 Cyber Resilience Conference (CRC), 2018, P. 1–4, doi: 10.1109/CR.2018.8626841.

7. V. Vasilyev, A. Kirillova, A. Vulfin and A. Nikonov, «Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score», 2021 International Conference on Information Technology and Nanotechnology (ITNT), 2021, P. 1–6, DOI: 10.1109/ITNT52450.2021.9649191.

СОБИНА Алена Александровна, магистрант Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: micropipe@gmail.com.

ЛИЗОВЕНКО Ольга Александровна, магистрант Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: lanuri@yandex.ru.

ПОНОМАРЕВА Ольга Алексеевна, Кандидат технических наук, Старший преподаватель Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: o.a.ponomareva@urfu.ru.

ЧЕРНОВА Ольга Вячеславовна, старший преподаватель Института радиоэлектроники и информационных технологий, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 32. E-mail: o.v.chernova@urfu.ru.

SOBINA Alena Aleksandrovna, Master's student of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: makkuropip@gmail.com.

LIZOVENKO Olga Aleksandrovna, Master's student of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: lanuri@yandex.ru.

PONOMAREVA Olga Alekseevna, Candidate of Technical Sciences, Senior Lecturer of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: o.a.ponomareva@urfu.ru.

CHERNOVA Olga Vjacheslavovna, Senior Lecturer of Institute of Radio Electronics and Information Technologies, Federal Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, st. Mira, 32. E-mail: o.v.chernova@urfu.ru.