Приложение 2
к Положению об
информационной безопасности

Методика оценки рисков

1. Общие положения

1. Методика оценки рисков информационной безопасности предназначена для проведения оценки рисков ИБ в рамках совершенствования системы СУИБ *в* НАО «Евразийский национальный университет» (далее Университет). Основная задача методики заключается в том, чтобы определить количественный показатель риска ИБ с целью принятия эффективных мер по защите информации. Методика определяет процесс идентификации, оценки и обработки рисков на основе любого нарушения конфиденциальности, персональности, целостности и доступности информационных ресурсов в рамках СУИБ в соответствии с международным стандартом ISO/IEC27001:2013. В этом документе описаны основные принципы методологии в отношении рисков информационной безопасности и процесса управления информационными рисками, а также связанных с ними любых ролей, обязанностей и деятельности.

2. Далее в документе описаны результаты оценки рисков информационной безопасности на основе разработанной методологии.

2. Термины и определения

3. БД - База данных, организованная в соответствии с определёнными правилами и поддерживаемая в памяти компьютера совокупность данных, характеризующая актуальное состояние некоторой предметной области и используемая для удовлетворения информационных потребностей пользователей

4. Бумажный документ - Рукописный или машинописный документ на бумаге.

5. Временная подписка - Договор по оказанию доступа к периодически обновляемым информационным продуктам, в течение определенного периода времени.

6. ИБ - Информационная Безопасность

7. Информационный актив - Материальный или нематериальный объект, который является информацией или содержит информацию, или необходим для обработки информации.

8. Конфиденциальные данные - Данные, относящиеся к операционной и финансово-хозяйственной деятельности организации.

9. Методология - Система принципов и способов организации и построения теоретической и практической деятельности.

10. СУИБ - Система управления информационной безопасности

11. Университет - НАО «Евразийский Национальный Университет»

12. Персональные данные - Сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе (из закона РК "О персональных данных и их защите")

13. Пользователи - Студенты, профессорско-преподавательский состав и иные категории сотрудников НАО «Евразийский Национальный Университет».

14. Электронная запись в базе данных - Информация, образовавшая в результате работы сотрудников в информационных системах и базах данных

15. Электронный документ - Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

16. **CIAP -** Параметры информации: конфиденциальность (C), целостность (I), доступность (A) и персональность (P) информационных ресурсов.

3. Описание методологии оценки рисков ИБ

17. Методология оценки рисков ИБ состоит из следующих этапов:

1) Этап 1. Идентификация активов;
2) Этап 2. Разработка модели угроз;
3) Этап 3. Оценка рисков.

4. Этап 1. Идентификация активов

18. На первом этапе оценки рисков ИБ осуществляется идентификация информационных активов Университета. Проводится интервью с сотрудниками каждого отдела/службы Университета, входящей в область действия СУИБ с целью выявления используемых активов.

5. Составление реестра информационных активов

19. По результатам проведенного анализа составляется Реестр активов согласно инструкции по категорированию активов Университета.

6. Определение владельцев активов

20. Для выявленных информационных активов определяются владельцы активов. Владельцы информационных активов — это лица (службы/отделы/департаменты), которые несут ответственность за защиту конкретных важных информационных активов. Владельцы могут делегировать задачи информационной безопасности менеджерам или другим лицам, но они несут ответственность за надлежащее выполнение задач и, в частности, отвечают за:

1) Соответствующую классификацию и защиту информационных активов;
2) Определение подходящих средств защиты;
3) Разрешение доступа к информационным ресурсам в соответствии с классификацией и потребностями бизнес-процессов Университета;

4) Обеспечение своевременного завершения регулярных обзоров доступа к системе / данным;

5) Контроль соблюдения требований защиты, влияющих на их активы.

7. Определение уровня конфиденциальности (C), целостности (I), доступности (A) и персональности (P) информационных ресурсов

21. Каждый информационный актив оценивается по параметрам CIAP. CIAP рассчитывается в количественной форме и выставляется путем присвоения баллов каждому активу. Уровни конфиденциальности, целостности и доступности определены следующими границами:

Таблица 1. Оценка параметров CIAP

Название атрибута	Значение	Коэффициент
Конфиденциальность данных (C)	Да	0.25
	Нет	0
Целостность данных (I)	Да	0.25
	Нет	0
Доступность данных (A)	Редко	0.075
	Ежедневно	0.15
	Часто	0.25
Персональность данных (P)	Да	0.25
	Нет	0

8. Определение атрибутов хранения

22. Для каждого выявленного информационного актива определяется ряд значений по следующим атрибутам хранения информационных ресурсов:

Таблица 2. Параметры хранения информации

№	Название атрибута	Значение
1	Хранение хотя бы на одном ПК	Да
		Нет
2	Актив можно найти в базах данных	Да
		Нет
3	Актив присутствует в бумажном виде	Да
		Нет
4	Для хранения/передачи актива используются переносные носители информации	Да
		Нет
5	Наличие персональных данных	Да
		Нет

23. В том числе происходит идентификация всех используемых мер по организации защиты выявленных активов и сроки по их архивации.

9. Категорирование и классификация

24. Целью категорирования информационных активов является удовлетворение требований законодательных и внутренних нормативных документов в области ИБ. Категорирование информационных активов осуществляется по следующей степени конфиденциальности:

Таблица 3. Классификация информации

№	Категория	Описание
1	Служебная	Сведения служебного характера, содержащиеся в различных видах документов, а также получаемые в процессе выполнения служебных функций.
2	Конфиденциальная	Данные, относящиеся к операционной и финансово-хозяйственной деятельности организации. Для более подробного списка конфиденциальной информации в Университете должен быть утвержден «Перечень конфиденциальной информации Университета»
3	Информация ограниченного распространения	Несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен.

25. Классификация информационных активов проводится по следующим категориям:

1) Бумажный документ;
2) Бумажный документ, электронная запись в базе данных, электронный документ;
3) Бумажный и электронный документ;
4) Временная подписка;
5) Электронная запись в базе данных;
6) Электронный документ.

10. Определение уровня возможных репутационных рисков от утечки / раскрытия информации

26. В ходе проводимой инвентаризации информационных активов Университета, устанавливается потенциальная величина ущерба, наносимого организации, в случае разглашения информации в соответствии со следующей классификацией уровня риска:

Таблица 4. Классификация величины ущерба

Величина ущерба	Описание	Коэффициент
Очень низкая	Материальный ущерб отсутствует, минимальное недовольство со стороны сотрудников и пользователей.	1
Низкая	Ущерб не материален, небольшое снижение уровня доверия со стороны сотрудников и пользователей.	2
Среднее	Ущерб меньше материальности, снижение уровня доверия со стороны сотрудников и пользователей, минимальные регуляторные санкции.	3
Высокая	Значительный ущерб больше материальности, потеря доверия некоторой части пользователей/партнеров, распространение негативной информации о компании в СМИ, регуляторные санкции, судебные издержки.	4
Катастрофическая	Банкротство и прекращение работы, невосстановимый ущерб для репутации, полная потеря доверия со стороны пользователей/партнеров и отказ работы с компанией, судебные преследования, существенные регуляторные санкции.	5

11. Определение вероятности возникновения риска

27. В ходе проведения интервью с владельцами информационных активов Университета, устанавливается потенциальная вероятность возникновения риска в соответствии со следующей классификацией вероятности возникновения риска:

Таблица 5. Классификация вероятности возникновения риска

Вероятность возникновения риска	Описание	Коэффициент
Очень низкая	Маловероятно	1
Низкая	Один раз в три года	2
Среднее	Один раз в год	3
Высокая	Несколько раз в год	4
Очень высокая	Раз в месяц и чаще	5

12. Этап 2. Разработка модели угроз

28. На данном этапе оценки разрабатывается модель основных угроз, с учетом определения вероятности наступления неблагоприятных событий и их актуальности. В ходе проведения анализа составляется перечень актуальных угроз на каждую идентифицированную группу активов, подверженных этим угрозам.

13. Этап 3. Оценка рисков

29. Для определения количественной величины идентифицированных рисков осуществляется расчёт согласно следующему алгоритму:

1. Расчет веса активов по атрибутам CIAP:

1) Вес конфиденциальности актива (C) = Балл по атрибуту конфиденциальности данных по заданной шкале;

2) Вес персональности актива (P) = Балл по атрибуту персональности данных по заданной шкале;

3) Вес целостности актива (I) = Балл по атрибуту целостности данных по заданной шкале;

4) Вес доступности актива (A) = Балл по атрибуту доступности данных по заданной шкале;

2. Расчет веса величины ущерба согласно заданной.

3. Расчет вероятности возникновения риска согласно заданной классификации.

4. Расчет совокупного балла оценочного показателя риска для каждого актива по формуле:

$$\text{Оценка риска} = \frac{\text{Коэффициент Вероятности} * \text{Коэффициент Величины ущерба} * (\text{C} + \text{I} + \text{A} + \text{P})}{25} * 100$$

При этом следует отметить, что наивысшее допустимое значение риска может составлять 25 баллов (т.е. 5*5*(0.25+0.25+0.25+0.25) = 25), в то время как результаты оценки риска отображаются в процентном соотношении для удобства интерпретации.

5. Расчет среднего балла оценочного показателя риска рассчитывается по заданной формуле:

$$\text{Средний бал} = \frac{\sum_{\text{N}}^{1} \text{Оценочный показатель риска каждого актива}}{\text{N}},$$

Где N – количество идентифицированных активов, подверженных данной угрозе.

6. Определение допустимого показателя риска.

Для оценки степени приемлемости риска определена зона риска в зависимости от ожидаемой величины потерь (Таблица 7).

Таблица 7. Зоны риска

Диапазон	Зона риска	Значение
> =15 баллов	Зона допустимого риска	К допустимому уровню риска отнесены те информационные риски, влияние которых на деятельность организации отсутствует либо оказывают незначительное влияние.
< 15 баллов	Зона критического риска	В зону критических рисков попадают информационные риски, влияние которых на деятельность организации может оказать существенный ущерб.

30. Информационные активы, идентифицированные в зоне допустимого риска, не требуют разработки для них дополнительных механизмов контроля. В то время как активы оценочный бал которых превышает 15 баллов требуют внимание и внедрение необходимых контролей для уменьшения вероятности возникновения либо влияния риска, в случае возникновения.

14. Заключение

31. Выполнение всех этапов проведения оценки рисков ИБ повторяется для каждого типа актива периодически. Полученное значение рисков ИБ необходимо для выработки рекомендаций по снижению уровня риска, а также принятия эффективных мер по обеспечению ИБ Университета.