Приложение 5
к Положению об
информационной безопасности

Правила проведения внутреннего аудита ИБ

1. Проведение аудита

1. Правила проведения внутреннего аудита ИБ НАО «Евразийский национальный университет им Л.Н. Гумилева» (далее - Университет) и ее мониторинга (далее - Правила) определяют порядок проведения проверок на соответствие требованиям информационной безопасности и работ по мониторингу информационной безопасности.

2. В Правилах используются понятия и определения, принятые в стандартах СТ РК 34.005-2002, СТ РК 34.006-2002, СТ РК 34.007-2002.

3. Проверки на предмет исполнения и соблюдения требований информационной безопасности разделяют на следующие виды проверок:

1) проверка ресурсов информационных систем, корпоративной вычислительной сети с целью подготовки технического задания на проектирование и разработку системы защиты информации;

2) проверка информационных систем, корпоративной вычислительной сети, после внедрения системы безопасности для оценки уровня ее эффективности;

3) профилактическая регулярная проверка, направленная на приведение действующей системы безопасности в соответствие требованиям нормативных правовых актов Республики Казахстан;

4) проверка, предназначенная для систематизации и упорядочивания существующих мер защиты информации;

5) проверка (служебное расследование) в целях расследования произошедшего инцидента, связанного с нарушением требований информационной безопасности;

6) совместная проверка, проводимая с компетентными государственными органами Республики Казахстан.

4. Проверки на предмет исполнения и соблюдения требований информационной безопасности подразделяются на плановые и внеплановые.

5. Плановые проверки на предмет исполнения и соблюдения требований информационной безопасности проводятся согласно утвержденному графику плановых проверок, который составляется ежегодно структурным подразделением, уполномоченным по обеспечению информационной безопасности – отделом информационной безопасности (далее - ОИБ) и утверждается Председателем Правления – Ректором Университета.

6. Процедура проведения плановой проверки включает в себя следующие мероприятия:

1) перед началом проверки, ОИБ вручает объекту проверки уведомление на проверку согласно приложению 1;

2) в уведомлении на проверку указываются срок уведомления, Ф.И.О. проверяющего, план проверки;

3) проверка проводится в соответствии с графиком проверок;

4) методы сбора информации включают интервьюирование сотрудников, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации, использование специализированных инструментальных средств;

5) после окончания проверки проводится анализ собранной информации, с целью оценки текущего уровня защищенности объекта проверки. По результатам проведенного анализа, руководству подразделения ответственного за объект проверки выдается рекомендация по устранению нарушений, согласно приложению 2.

7. Внеплановые проверки на предмет исполнения и соблюдения требований информационной безопасности проводятся на основании составленных актов о выявленных нарушениях согласно приложению 3 с резолюцией руководства Университета, компетентных органов.

8. При проведении проверок (плановых и внеплановых) сотрудники ОИБ имеют право:

1) приглашать руководителей структурных подразделений и сотрудников Университета для выяснения вопросов по выявленным нарушениям и недостаткам, получать от них письменные объяснения на имя руководства Университета и истребовать материалы;

2) запрашивать и получать от всех структурных подразделений Университета документы (справки, заключения и другие материалы), касающиеся организации и порядка проведения информационного аудита, проверок, эксплуатации автоматизированного оборудования и программного обеспечения, а также соблюдения требований информационной безопасности;

3) вносить для рассмотрения руководству Университета предложения по результатам проверок, проведенных в структурных подразделениях;

4) иметь беспрепятственный доступ во все служебные помещения структурных подразделений Университета, а также:

- в помещения, где установлено оборудование корпоративной сети, серверные, телекоммуникации.

2. Проведение мониторинга

9. Мониторинг информационной безопасности осуществляется ОИБ.

10. В задачи мониторинга информационной безопасности входит контроль за соблюдением политики информационной безопасности и требованиям гармонизированному стандарту Республики Казахстан СТ РК ИСО/МЭК 17799-2006.

11. Сотрудниками ОИБ должен проводиться мониторинг следующих процессов:

1) контроль информационных потоков и сообщений от сетевых экранов;

2) контроль операционных систем и открываемых портов;

3) выявление попыток несанкционированного доступа (НСД);

4) выявление уязвимых мест в ЛВС Университета и рекомендации по их защите;

5) выявление и анализ событий, содержащих информацию о подозрительной активности (события безопасности);

6) контроль общей активности пользователей;

7) контроль выделенных подключений к глобальной сети;

8) учет и мониторинг зарегистрированных пользователей ЛВС Университета.

12. Мониторинг должен проводиться при помощи специализированных лицензионных аппаратно-программных средств защиты информации.

13. Периодичность мониторинга устанавливается начальником ОИБ и зависит от используемого программного или программно-аппаратного обеспечения.

14. Результаты деятельности (отчет) по мониторингу должны представляться начальнику ОИБ.

15. По представленному отчету должен проводиться анализ. При выявлении фактов нарушения информационной безопасности составляется акт о выявленных нарушениях и докладывается руководству Университета.

Приложение 1
к Правилам проведения
внутреннего аудита ИБ

Уведомление № _____
о проведении проверки на предмет исполнения и соблюдения требований информационной безопасности

«___» _____ 20___ года

1. _____
(полное наименование объекта)

2. _____
(цель проверки)

_____
_____
_____
_____
_____

3. Должность, Ф.И.О. уполномоченных на проведение проверки

_____
_____
_____
_____
_____

4. Срок проведения проверки_____

Начальник отдела
информационной безопасности _____
_____
(подпись) (Ф.И.О.)

Приложение 2
к Правилам проведения
внутреннего аудита ИБ

**Рекомендации по устранению выявленных нарушений
по информационной безопасности**

Настоящие рекомендации выданы
_____
(кем выдано)
_____
_____
На основании проведенной проверки от «___» _____ 20___ г.
Согласно уведомлению на проведение проверки от «___» _____ 20___ г.,
№
_____
(наименование подразделения)
Выявленные нарушения и рекомендации по устранению:
_____
_____
_____
_____
_____
_____
(подпись должность, проверяющего) (Ф.И.О.)

Приложение 3
к Правилам проведения
внутреннего аудита ИБ

Акт о выявленных нарушениях

№ _____ от «___ _____ 20___ г.

Место проведения проверки
_____

Должности, Ф.И.О. должностных лиц, проводивших проверку
_____
_____
_____

Полное наименование объекта проверки
_____
_____
_____

Выявлены нарушения:
_____
_____
_____
_____

Должность лица,
проводившего проверку _____
_____
(подпись) (Ф.И.О.)

Должность проверяемого лица _____
_____
(подпись) (Ф.И.О.)