

**kaspersky**

Утверждено:

██████████  
██████████

Подпись:

Дата публикации: 01/12/2021

Дата вступления в силу: 24/11/2021

# **Политика безопасности при использовании бионических устройств**

Политика безопасности при использовании бионических устройств		КОД ДОКУМЕНТА
Дата вступления в силу: 24.11.2021	Дата следующего пересмотра: 24.11.2022	Версия: 1

## Цель документа

Настоящая политика регулирует порядок использования бионических устройств в «Лаборатории Касперского» (далее - ЛК) и направлена на снижение рисков, связанных со спецификой таких устройств и особенностью их применения в бизнес-процессах ЛК.

Данный документ предлагает ряд процессов стандартизации, повышающих безопасность и обеспечивающих более инклюзивную рабочую среду для сотрудников, использующих бионические устройства. Политика является публичным документом с целью привлечения мирового ИТ-сообщества к обсуждению и к объединению усилий по дальнейшим шагам к достижению безопасности использования бионических устройств, например, таким, как обеспечение цифровой конфиденциальности данных на устройствах, предоставление различных уровней доступа к хранимой информации или анализ потенциальных рисков и угроз, связанных со здоровьем человека.

Контакт для обсуждения дальнейших вопросов и идей для сотрудничества: [augmentedfuture@kaspersky.com](mailto:augmentedfuture@kaspersky.com)

## Область действия и сфера применения

Настоящий документ используется на уровне Компании и применяется ко всем ее структурным подразделениям. Настоящая Политика применяется ко всей СКУД, а также процессам администрирования, сопровождения и использования автоматизированных систем ЛК. Политика распространяется на всех сотрудников и временный персонал ЛК, а также сотрудников сторонних организаций, оказывающие ЛК согласованные услуги, и является обязательной для исполнения.

## Определения

- Бионическое устройство - устройство, заменяющие или дополняющие части тела человека искусственными устройствами - имплантами. К данным устройствам относятся:
  - Чип-имплант (вживленный в тело/кожу)
    - NFC-биочип – чип-имплант, поддерживающее передачу информации посредством технологии NFC, вживленное в кожу человека
  - Бионические импланты конечностей (руки/ноги) и внутренних органов
  - Искусственные органы чувств (зрачки, слуховые аппараты)
- СКУД – система контроля управления доступом

## Использование различных бионических устройств внутри ЛК

### NFC-биочип

Из бионических устройств в ЛК чаще всего используются NFC-биочипы, которые выполняют роль идентификации сотрудника в системе СКУД, при поднесении к считывателю турникета (вместо привычных всем карточек сотрудника). Рассмотрим различные зоны безопасности в ЛК и порядок получения доступа к различным уровням с помощью NFC-биочипа.

Политика безопасности при использовании бионических устройств		КОД ДОКУМЕНТА
Дата вступления в силу: 24.11.2021	Дата следующего пересмотра: 24.11.2022	Версия: 1

## Порядок прохождения зон безопасности

В ЛК установлены 4 зоны безопасности:

- Зеленая - прилегающие территории к офисному зданию, на которой могут располагаться автотранспортные средства работников и гостей, площадки для дизельных генераторов, а также зоны погрузки-выгрузки.
- Желтая - холлы и помещения до турникетов.
- Синяя - холлы и помещения, находящиеся за турникетами, а также подземный паркинг.
- Красная - охраняемые помещения, доступ в которые строго ограничен. Доступ в такие помещения регулируется Процедурой доступа в охраняемые помещения. К таким помещениям могут относиться ЦОД, серверные, складские помещения и другие чувствительные места, куда следует ограничить доступ рядового сотрудника.

Доступ к «зеленому» и «желтому» уровню безопасности не требует идентификации личности и наличие пропуска (в т.ч. гостевого).

При получении доступа к «синему» уровню безопасности на турникетах следует предъявить NFC-биочип к считывающему устройству на турникетах. Номер чипа заносится в контроллер СКУД при поступлении на работу и в нем указывается права на посещения объектов.

Для получения новых доступов внутри «синей» и доступа в «красную» зоны следует написать запрос в Service Desk. При запросе доступа следует указать бизнес-основания его получения. Также для физического доступа в некоторые части офиса ЛК для идентификации сотрудников в системе СКУД допустимы следующие методы подтверждения личности:

- Распознавание голоса
- Отпечаток пальцев

Более подробно о разделении офиса на зоны безопасности: [Положение о пропускном и внутриобъектовом режиме.](#)

Токен для временного или гостевого пропуска для NFC-биочипа не предоставляется.

Запрещено:

- Предоставлять доступ постороннему человеку или сотруднику в офис с помощью собственного NFC-биочипа

При получении санкционированного или несанкционированного доступа к NFC-биочипу следует незамедлительно уведомить отдел ИБ.

## Процесс обновления сервисов

Для всех бионических устройств, присутствующих в Компании, следует проводить процедуру обновления сервисов (patch-management), выполняя следующее SLA (Service Level Agreement):

- Критичные обновления (CVSS > 7):
  - при запросе от отдела ИБ или Product Security - минимально возможный срок (до 1 недели с выхода обновления);
  - в плановом режиме - 30 дней с даты выхода обновления в канал обновления вендора или установки ресурса.
- Важные обновления (CVSS > 5):
  - 30 дней с даты выхода обновления в канал обновления вендора или установки ресурса.

Политика безопасности при использовании бионических устройств		КОД ДОКУМЕНТА
Дата вступления в силу: 24.11.2021	Дата следующего пересмотра: 24.11.2022	Версия: 1

- Некритичные обновления (CVSS  $\leq$  5):
  - 90 дней с даты выхода обновления в канал обновления вендора или установки ресурса.

При невозможности установки обновлений (например, если обновление вызывает проблемы в эксплуатации) следует согласовать исключение с отделом ИБ, а также митигировать риски, вызванные неактуальной версией ПО, другими методами.

### **Увольнение сотрудника**

При увольнении все доступы, которые имел сотрудник, должны быть удалены из системы СКУД.

### **Требования к NFC-биочипу**

NFC-биочип должен обладать следующими характеристиками:

1. Объем памяти не менее 1kb
2. Размер уникального ID не менее 32 символов
3. Не менее двух блоков памяти, каждый из которых имеет свой ключ и уровень доступа
4. Поддержка надежных криптографических стандартов шифрования (AES, ГОСТ 34.12-2018 и тд.)

## **Бионические импланты конечностей, внутренних органов и искусственных органов чувств**

Для бионических имплантов конечностей (руки/ноги), внутренних органов (например, кардиостимулятор) и искусственных органов чувств (искусственные зрачки, слуховые аппараты) внутри ЛК нет ограничений на использование.

### **Прохождение металлодетектора сотрудниками с бионическими имплантами**

Сотрудники, имеющие бионические импланты конечностей и внутренних органов, освобождаются от обязанности прохождения металлодетектора. Для подтверждения наличия бионического импланта (например, кардиостимулятора) следует предоставить сотруднику СБ выписку от врача.

### **Организация рабочего места для сотрудников с искусственными органами чувств**

Для сотрудников, имеющих искусственные органы чувств, следует по-особому организовывать рабочие места, в частности использовать разделение между отделами и сотрудниками (например, перегородки) для исключения возможной утечки конфиденциальной информации по аудиовизуальным каналам. Перегородки должны быть затемнены и не пропускать шум.

## **Ограничения для некоторых видов бионических устройств**

Для бионических устройств, имеющих некоторый функционал, предназначенный для негласного получения информации (например, умеет скрытно записывать аудио- или видеофайлы; имеет встроенные интерфейсы, такие как GPS, Wi-Fi), следует заранее уведомлять отдел ИБ для согласования или отдел HR при приеме на работу. Следует узнать и указать модель бионического устройства для уточнения спецификаций.

Политика безопасности при использовании бионических устройств		КОД ДОКУМЕНТА
Дата вступления в силу: 24.11.2021	Дата следующего пересмотра: 24.11.2022	Версия: 1

## **Безопасность при работе в местах с повышенным электромагнитным излучением**

Для сотрудников с бионическими имплантами ограничен доступ в помещения с повышенным уровнем излучения (более 6.5 В/м). Сотрудники должны быть проинформированы о запрете посещения этих мест.

## **Ответственность при невыполнении требований**

Нарушение или невыполнение вышеперечисленных требований несет следующие риски для ЛК:

- Кража конфиденциальной информации
- Кража биометрической и медицинской информации
- Проникновение злоумышленника на территорию ЛК
- Распространение информации, не предназначенной для общественности
- Ущерб репутации ЛК
- Прямые финансовые потери

Нарушение или невыполнение сотрудниками ЛК вышеперечисленных требований Политики влечет за собой применение мер дисциплинарного характера.

Политика безопасности при использовании бионических устройств		КОД ДОКУМЕНТА
Дата вступления в силу: 24.11.2021	Дата следующего пересмотра: 24.11.2022	Версия: 1

## Лист регистрации изменений

Вер.	Действие (и описание изменений)	Дата	Ответственный	Статус
1	Закончена разработка документа	24.11.2021	██████████	Выполнено

## Согласующие лица

№	Согласующее лицо	Дата	Подпись
1	██████████	24.11.2021	
2	██████████	24.11.2021	
3	██████████	24.11.2021	
4	██████████	24.11.2021	

[www.kaspersky.com/](http://www.kaspersky.com/)  
[www.securelist.com](http://www.securelist.com)