



МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова»  
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

**П Р И К А З**

24.07.2023

№ 564-0

Санкт-Петербург

**Об утверждении положений об управлении безопасности и его  
структурных подразделений**

В соответствии с пунктом 3.4 устава федерального государственного бюджетного образовательного учреждения «ВОЕНМЕХ» им. Д.Ф. Устинова» (далее – Университет) в целях определения правового статуса, функций и полномочий структурных подразделений Университета

**приказываю:**

1. Утвердить и ввести в действие положение об управлении безопасности БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова (Приложение № 1).
2. Утвердить и ввести в действие положение об отделе оперативной полиграфии БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова (Приложение № 2).
3. Утвердить и ввести в действие положение об отделе информационной и кибербезопасности БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова (Приложение № 3).
4. Советнику по безопасности ректората, исполняющему обязанности начальника управления безопасности Байкову А.Т. обеспечить ознакомление под подпись подчиненных работников с положением об управлении безопасности БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.
5. Начальнику отдела оперативной полиграфии Перекотиенко А.М. обеспечить ознакомление под подпись подчиненных работников с положением об отделе оперативной полиграфии БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.
6. Начальнику отдела информационной и кибербезопасности Чапрасову В.С. обеспечить ознакомление под подпись подчиненных

Приложение № 1  
к приказу от 24.07.2023 № 564-0

Федеральное государственное бюджетное образовательное учреждение высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»  
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

УТВЕРЖДЕНО  
приказом ректора  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова  
от 24.07 - 2023 г. № 564-0

**ПОЛОЖЕНИЕ**  
**об управлении безопасности**  
**БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова**

Санкт-Петербург  
2023

## Оглавление

1. Общие положения.....	3
2. Цели и задачи деятельности подразделения.....	4
3. Структура подразделения.....	5
4. Функции подразделения.....	5
5. Права подразделения.....	8
6. Взаимоотношения и связи подразделения .....	8
7. Ответственность подразделения .....	9

## 1. Общие положения

1.1. Положение об управлении безопасности БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова (далее – Положение) регламентирует деятельность, цели, задачи, функции, права, ответственность управления безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» (далее – Университет), а также его взаимодействие с другими структурными подразделениями Университета.

1.2. Управление безопасности непосредственно подчинено ректору Университета.

1.3. Общее руководство управлением безопасности осуществляет начальник управления, который непосредственно подчинен ректору Университета.

1.4. Управление безопасности реорганизуется и ликвидируется приказом ректора Университета.

1.5. В своей деятельности управление безопасности руководствуется:

- Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами государственных органов по защите государственной тайны, в том числе нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности;

- нормативными правовыми актами Министерства науки и высшего образования Российской Федерации;

- Уставом Университета;

- политикой и целями Университета в области качества;

- локальными нормативными документами Университета;

- правилами охраны труда, промышленной и пожарной безопасности, иными требованиями обеспечения безопасности жизни и здоровья работников Университета;

- настоящим Положением.

1.6. Финансирование деятельности управления безопасности осуществляется за счет средств субсидий, выделенных на выполнение государственного задания, внебюджетных средств Университета и иных источников финансирования, предусмотренных законодательством Российской Федерации и уставом Университета.

## **2. Цели и задачи деятельности подразделения**

2.1. Основными целями управления безопасности являются:

2.1.1. Исключение или существенное снижение негативных последствий (ущерба) в отношении Университета вследствие нарушения функционирования его информационных и автоматизированных систем, информационно-телекоммуникационных сетей в результате реализации угроз безопасности информации.

2.1.2. Обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

2.1.3. Повышение защищенности Университета от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных (автоматизированных) систем Университета или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования.

2.1.4. Обеспечение надежности, а также эффективности функционирования и безопасности информационных систем Университета.

2.1.5. Обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем, информационно-телекоммуникационной сети и автоматизированных систем управления Университета.

2.1.6. Удовлетворение потребностей структурных подразделений Университета в издании учебной, учебно-методической, научной литературы, изготовлении бланочной продукции, размножении технической и служебно-распорядительной документации содержащих информацию ограниченного доступа.

2.2. Основными задачами управления безопасности являются:

2.2.1. В части обеспечения информационной безопасности Университета:

- планирование, организация и координация работ по обеспечению информационной безопасности, контроль за ее состоянием в Университете;

- выявление угроз безопасности информации и уязвимостей информационных (автоматизированных) систем, программного обеспечения и программно-аппаратных средств;

- предотвращение утечки конфиденциальной информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

- поддержание стабильной деятельности Университета в случае проведения компьютерных атак;

- обеспечение безопасности функционирования информационных (автоматизированных) систем, образовательного и производственных процессов Университета;

- взаимодействие с Национальным координационным центром по компьютерным инцидентам;

- организация нормативно-правового обеспечения использования информационных ресурсов.

2.2.2. В части издания литературы, изготовления бланочной продукции, размножения технической и служебно-распорядительной документации ограниченного доступа:

- тиражирование учебных, учебно-методических, научных, информационных и иных материалов, служебно-распорядительных документов, технической документации, содержащих информацию ограниченного доступа.

- изготовление бланочной продукции Университета, содержащей информацию ограниченного доступа;

- контроль качества выпускаемой полиграфической продукции.

- совершенствование организации процесса производства полиграфической продукции, его технологий, повышение качества выполняемых работ, снижение трудоемкости и себестоимости изготовления полиграфической продукции.

### **3. Структура подразделения**

3.1. В состав управления безопасности входят:

- отдел информационной и кибербезопасности;

- отдел оперативной полиграфии.

### **4. Функции подразделения**

4.1. В соответствии с поставленной целью для решения основных задач по обеспечению информационной безопасности Университета управление безопасности выполняет следующие основные функции:

4.1.1. Разрабатывает планы работ по обеспечению информационной безопасности в Университете, осуществляет его координацию и контроль выполнения.

4.1.2. Разрабатывает предложения по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Университете, представляет их ректору Университета.

4.1.3. Выявляет и проводит анализ угроз безопасности информации в отношении Университета, уязвимости информационных систем, программного обеспечения, программно-аппаратных средств и принимает меры по их устранению.

4.1.4. Обеспечивает в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработку и реализацию организационных мер, и применение средств обеспечения информационной безопасности в Университете.

4.1.5. Обнаруживает, предупреждает и ликвидирует последствия компьютерных атак и реагирует на компьютерные инциденты.

4.1.6. Предоставляет в Национальный координационный центр по компьютерным инцидентам информацию о выявленных компьютерных инцидентах в Университете.

4.1.7. Исполняет указания Федеральной службы безопасности Российской Федерации (ФСБ России) и ее территориальных органов, Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Министерства науки и высшего образования Российской Федерации (Минобрнауки России) по результатам мониторинга защищенности информационных ресурсов, принадлежащих Университету либо используемых Университетом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет».

4.1.8. Проводит анализ и контроль за состоянием защищенности систем и сетей и разрабатывает предложения по модернизации (трансформации) основных процессов Университета в целях обеспечения информационной безопасности.

4.1.9. Осуществляет подготовку отчетов о состоянии работ по обеспечению информационной безопасности в Университете.

4.1.10. Выполняет функции администраторов информационной безопасности Университета по предотвращению несанкционированного доступа лиц к защищаемой информации в информационных системах Университета.

4.1.11. Контролирует предоставление и отзыв прав доступа к информационным ресурсам в Университете.

4.1.12. Осуществляет мониторинг действий пользователей в процессе их работы в информационных системах Университета.

4.1.13. Учитывает и контролирует события, связанные с информационной безопасностью Университета.

4.1.14. Контролирует удаленный доступ к информационной инфраструктуре Университета.

4.1.15. Контролирует настройки сетевого оборудования в соответствии с требованиями информационной безопасности Университета.

4.1.16. Контролирует состояния антивирусной защиты информационных систем Университета.

4.1.17. Осуществляет мониторинг действий пользователей в информационных системах Университета.

4.1.18. Участвует в действиях по восстановлению работоспособности оборудования, обеспечивающего информационную безопасность Университета, после сбоев и аварий.

4.1.19. Согласовывает технические задания, проектную и другую техническую документацию на вновь создаваемые информационные системы или программное обеспечение, услуги в области информационных технологий в части выполнения требований по защите информации.

4.1.20. Осуществляет проведение плановых проверок режима защиты информации, обеспечивает разработку соответствующей документации, проводит анализ результатов и расследование нарушений.

4.1.21. Организует и проводит мероприятия по повышению осведомленности работников и обучающихся Университета по вопросам обеспечения информационной безопасности.

4.1.22. Обеспечивает информационную поддержку работников Университета по вопросам информационной безопасности.

4.1.23. Организует внедрение нормативных документов по обеспечению информационной безопасности в Университете.

4.2. В соответствии с поставленной целью для решения основных задач по изданию литературы, изготовлению бланочной продукции, размножению технической и служебно-распорядительной документации ограниченного доступа управление безопасности выполняет следующие основные функции:

4.2.1. Прием учебных, учебно-методических, научных, информационных и иных материалов, служебно-распорядительных документов, технической документации для копирования и тиражирования.

4.2.2. Обеспечение учета и сохранности принятых в работу учебных, учебно-методических, научных, информационных и иных материалов, служебно-распорядительных документов, технической документации, содержащих информацию ограниченного доступа, в соответствии с установленными в Университете требованиями.

4.2.3. Своевременное и качественное выполнение копировальных и множительных работ, и учет расхода используемых материалов.

4.2.4. Эксплуатация, хранение и поддержание печатной, бумагорезательной, копировальной и др. техники отдела в соответствии с технической документацией на оборудование и требованиями по безопасности информации.

4.2.5. Ведение учета материальных средств и расходных материалов.

4.2.6. Ведение секретного и конфиденциального делопроизводства в соответствии с номенклатурой Университета.



4.3. Осуществление в пределах своей компетенции иных функций в соответствии с основными задачами управления безопасности.

## **5. Права подразделения**

С целью реализации функций управление безопасности имеет право:

5.1. Запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений Университета, необходимым для принятия решений по всем вопросам, отнесенным к компетенции управления.

5.2. Готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности Университета, имеющих лицензии на соответствующий вид деятельности.

5.3. Контролировать деятельность структурных подразделений Университета по выполнению требований по обеспечению информационной безопасности.

5.4. Постоянно повышать профессиональные компетенции, знания и навыки работников управления.

5.5. Участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций.

5.6. Участвовать в работе комиссий Университета в пределах своих компетенций.

5.7. Проводить плановые и внеплановые проверки структурных подразделений Университета по выполнению требований по обеспечению информационной безопасности.

5.8. Вносить предложения ректору Университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности.

5.9. Вносить представления ректору Университета в отношении работников при обнаружении фактов нарушения работниками Университета установленных требований безопасности информации в Университете, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности.

5.10. Привлекать в случае необходимости на договорной основе независимых специалистов по ремонту копировально-множительной техники.

5.11. Вносить на рассмотрение ректору Университета предложения по вопросам деятельности управления.

## **6. Взаимоотношения и связи подразделения**

6.1. В своей деятельности управление безопасности осуществляет служебные взаимоотношения и поддерживает связи со всеми структурными

подразделениями Университета с целью обмена информацией и документами, а также выполнения возложенных на управление безопасности задач.

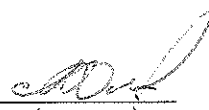
## **7. Ответственность подразделения**

7.1. Ответственность за своевременное и качественное выполнение установленных настоящим Положением задач и функций несет начальник управления.

7.2. Степень ответственности работников управления указана в соответствующих должностных инструкциях.

Разработано:

Советник по безопасности Ректората –  
исполняющий обязанности начальника  
управления безопасности

  
\_\_\_\_\_

(подпись)

\_\_\_\_\_

(дата)

А.Т. Байков

**Лист ознакомления  
с положением об управлении безопасности  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова**

Должность	ФИО	Дата	Подпись

<b>Должность</b>	<b>ФИО</b>	<b>Дата</b>	<b>Подпись</b>

Приложение № 2  
к приказу от 24.07.2023 № 564-0

Федеральное государственное бюджетное образовательное учреждение высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»  
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

УТВЕРЖДЕНО  
приказом ректора  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова  
от 24.07 2023 г. № 564-0

**ПОЛОЖЕНИЕ**  
**об отделе оперативной полиграфии**  
**БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова**

Санкт-Петербург  
2023

## Оглавление

1. Общие положения .....	3
2. Цели и задачи деятельности подразделения.....	3
3. Структура подразделения.....	4
4. Функции подразделения.....	4
5. Права подразделения.....	5
6. Взаимоотношения и связи подразделения .....	5
7. Ответственность подразделения .....	5

## **1. Общие положения**

1.1. Положение об отделе оперативной полиграфии БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова (далее – Положение) регламентирует деятельность, цели, задачи, функции, права, ответственность отдела оперативной полиграфии Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» (далее – Университет), а также его взаимодействие с другими структурными подразделениями Университета.

1.2. Отдел оперативной полиграфии непосредственно подчинен начальнику управления безопасности Университета.

1.3. Общее руководство отделом оперативной полиграфии осуществляет начальник отдела, который непосредственно подчинен начальнику управления безопасности Университета.

1.4. Отдел оперативной полиграфии реорганизуется и ликвидируется приказом ректора Университета.

1.5. В своей деятельности отдел оперативной полиграфии руководствуется:

- Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, нормативными правовыми актами государственных органов по защите государственной тайны, в том числе нормативными документами по полиграфической деятельности;

- нормативными правовыми актами Министерства науки и высшего образования Российской Федерации;

- Уставом Университета;

- Коллективным договором;

- локальными нормативными документами Университета;

- правилами охраны труда, промышленной и пожарной безопасности, иными требованиями обеспечения безопасности жизни и здоровья работников Университета.

- настоящим Положением.

1.6. Финансирование деятельности отдела оперативной полиграфии осуществляется за счет средств субсидий, выделенных на выполнение государственного задания, внебюджетных средств Университета и иных источников финансирования, предусмотренных законодательством Российской Федерации и уставом Университета.

## **2. Цели и задачи деятельности подразделения**

2.1. Основными целями отдела оперативной полиграфии являются:

2.1.1. Удовлетворение потребностей структурных подразделений Университета в издании учебной, учебно-методической, научной литературы, изготовлении бланочной продукции, размножении технической и служебно-распорядительной документации содержащих информацию ограниченного доступа.

2.1.2. Обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

2.2. Основными задачами отдела оперативной полиграфии являются:

2.2.1. Тиражирование учебных, учебно-методических, научных, информационных и иных материалов, служебно-распорядительных документов, технической документации, содержащих информацию ограниченного доступа.

2.2.2. Изготовление бланочной продукции Университета, содержащей информацию ограниченного доступа.

2.2.3. Контроль качества выпускаемой полиграфической продукции.

2.2.4. Совершенствование организации процесса производства полиграфической продукции, его технологий, повышение качества выполняемых работ, снижение трудоемкости и себестоимости изготовления полиграфической продукции.

### **3. Структура подразделения**

3.1. Организационная структура и штатная численность отдела оперативной полиграфии утверждается приказом ректора Университета по представлению начальника управления безопасности.

3.2. Работники отдела оперативной полиграфии назначаются на должность и освобождаются от нее приказом ректора Университета по представлению начальника управления безопасности.

3.3. Распределение обязанностей между работниками отдела оперативной полиграфии осуществляется начальником отдела.

### **4. Функции подразделения**

В соответствии с поставленной целью для решения основных задач отдел оперативной полиграфии выполняет следующие основные функции:

4.1. Прием учебных, учебно-методических, научных, информационных и иных материалов, служебно-распорядительных документов, технической документации для копирования и тиражирования.

4.2. Обеспечение учета и сохранности принятых в работу учебных, учебно-методических, научных, информационных и иных материалов, служебно-распорядительных документов, технической документации, содержащих информацию ограниченного доступа, в соответствии с установленными в Университете требованиями.

4.3. Своевременное и качественное выполнение копировальных и множительных работ, и учет расхода используемых материалов.

4.4. Эксплуатация, хранение и поддержание печатной, бумагорезательной, копировальной и др. техники отдела в соответствии с технической документацией на оборудование и требованиями по безопасности информации.

4.5. Ведение учета материальных средств и расходных материалов.

4.6. Ведение секретного и конфиденциального делопроизводства в соответствии с номенклатурой Университета.



4.7. Осуществление в пределах своей компетенции иных функций в соответствии с основными задачами управления безопасности.

## **5. Права подразделения**

С целью реализации функций отдел оперативной полиграфии имеет право:

5.1. Получать в установленном порядке документы и материалы структурных подразделений Университета, необходимые для выполнения задач, отнесенных к компетенции отдела.

5.2. Привлекать в случае необходимости на договорной основе независимых специалистов по ремонту копировально-множительной техники.

5.3. Вносить на рассмотрение руководству управления безопасности предложения по вопросам деятельности отдела.

## **6. Взаимоотношения и связи подразделения**

6.1. В своей деятельности отдел оперативной полиграфии осуществляет служебные взаимоотношения и поддерживает связи со всеми структурными подразделениями Университета с целью обмена информацией и документами, а также выполнения возложенных на отдел задач.

## **7. Ответственность подразделения**

7.1. Ответственность за своевременное и качественное выполнение установленных настоящим Положением задач и функций несет начальник отдела оперативной полиграфии.

7.2. Степень ответственности работников отдела оперативной полиграфии указана в соответствующих должностных инструкциях.

Разработано:

Начальник отдела оперативной полиграфии



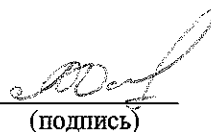
(подпись)

(дата)

А.М. Перекотиенко

Согласовано:

Советник по безопасности Ректората –  
исполняющий обязанности начальника  
управления безопасности



(подпись)

(дата)

А.Т. Байков

**Лист ознакомления  
с положением об отделе оперативной полиграфии  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова**

Должность	ФИО	Дата	Подпись

Приложение № 3  
к приказу от 24.07.2023 № 564-0

Федеральное государственное бюджетное образовательное учреждение высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»  
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

УТВЕРЖДЕНО  
приказом ректора  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова  
от 24.07 2023 г. № 564-0

**ПОЛОЖЕНИЕ**  
**об отделе информационной и кибербезопасности**  
**БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова**

Санкт-Петербург  
2023

## Оглавление

1. Общие положения .....	3
2. Цели и задачи деятельности подразделения .....	4
3. Структура подразделения .....	5
4. Функции подразделения .....	5
5. Права подразделения .....	7
6. Взаимоотношения и связи подразделения .....	8
7. Ответственность подразделения .....	8

## **1. Общие положения**

1.1. Положение об отделе информационной и кибербезопасности БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова (далее – Положение) регламентирует деятельность, цели, задачи, функции, права, ответственность отдела информационной и кибербезопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» (далее – Университет), а также его взаимодействие с другими структурными подразделениями Университета.

1.2. Отдел информационной и кибербезопасности непосредственно подчинен начальнику управления безопасности Университета.

1.3. Общее руководство отделом информационной и кибербезопасности осуществляет начальник отдела, который непосредственно подчинен начальнику управления безопасности Университета.

1.4. Отдел информационной безопасности реорганизуется и ликвидируется приказом ректора Университета.

1.5. В своей деятельности отдел информационной и кибербезопасности руководствуется:

- Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности;

- нормативными правовыми актами Министерства науки и высшего образования Российской Федерации;

- Уставом Университета;

- политикой и целями Университета в области качества;

- локальными нормативными документами Университета;

- правилами охраны труда, промышленной и пожарной безопасности, иными требованиями обеспечения безопасности жизни и здоровья работников Университета.

- настоящим Положением.

1.6. Финансирование деятельности отдела информационной и кибербезопасности осуществляется за счет средств субсидий, выделенных на выполнение государственного задания, внебюджетных средств Университета и иных источников финансирования, предусмотренных законодательством Российской Федерации и уставом Университета.

## **2. Цели и задачи деятельности подразделения**

2.1. Основными целями отдела информационной и кибербезопасности являются:

2.1.1. Исключение или существенное снижение негативных последствий (ущерба) в отношении Университета вследствие нарушения функционирования его информационных и автоматизированных систем, информационно-телекоммуникационных сетей в результате реализации угроз безопасности информации.

2.1.2. Обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

2.1.3. Повышение защищенности Университета от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных (автоматизированных) систем Университета или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования.

2.1.4. Обеспечение надежности, а также эффективности функционирования и безопасности информационных систем Университета.

2.1.5. Обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем, информационно-телекоммуникационной сети и автоматизированных систем управления Университета.

2.2. Основными задачами отдела информационной и кибербезопасности являются:

2.2.1. Планирование, организация и координация работ по обеспечению информационной безопасности, контроль за ее состоянием в Университете.

2.2.2. Выявление угроз безопасности информации и уязвимостей информационных (автоматизированных) систем, программного обеспечения и программно-аппаратных средств.

2.2.3. Предотвращение утечки конфиденциальной информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

2.2.4. Поддержание стабильной деятельности Университета в случае проведения компьютерных атак.

2.2.5. Обеспечение безопасности функционирования информационных (автоматизированных) систем, образовательного и производственных процессов Университета.

2.2.6. Взаимодействие с Национальным координационным центром по компьютерным инцидентам.

2.2.7. Организация нормативно-правового обеспечения использования информационных ресурсов.

### **3. Структура подразделения**

3.1. Организационная структура и штатная численность отдела информационной и кибербезопасности утверждается приказом ректора Университета по представлению начальника управления безопасности.

3.2. Работники отдела информационной и кибербезопасности назначаются на должность и освобождаются от нее приказом ректора Университета по представлению начальника управления безопасности.

3.3. Распределение обязанностей между работниками отдела информационной и кибербезопасности осуществляется начальником отдела.

### **4. Функции подразделения**

В соответствии с поставленной целью для решения основных задач отдел информационной и кибербезопасности выполняет следующие основные функции:

4.1. Разрабатывает планы работ по обеспечению информационной безопасности в Университете, осуществляет его координацию и контроль выполнения.

4.2. Разрабатывает предложения по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Университете, представляет их начальнику управления безопасности.

4.3. Выявляет и проводит анализ угроз безопасности информации в отношении Университета, уязвимости информационных систем, программного обеспечения, программно-аппаратных средств и принимает меры по их устранению.

4.4. Обеспечивает в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработку и реализацию организационных мер, и применение средств обеспечения информационной безопасности в Университете.

4.5. Обнаруживает, предупреждает и ликвидирует последствия компьютерных атак и реагирует на компьютерные инциденты.

4.6. Предоставляет в Национальный координационный центр по компьютерным инцидентам информацию о выявленных компьютерных инцидентах в Университете.

4.7. Исполняет указания Федеральной службы безопасности Российской

Федерации (ФСБ России) и ее территориальных органов, Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Министерства науки и высшего образования Российской Федерации (Минобрнауки России) по результатам мониторинга защищенности информационных ресурсов, принадлежащих Университету либо используемых Университетом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет».

4.8. Проводит анализ и контроль за состоянием защищенности систем и сетей и разрабатывает предложения по модернизации (трансформации) основных процессов Университета в целях обеспечения информационной безопасности.

4.9. Осуществляет подготовку отчетов о состоянии работ по обеспечению информационной безопасности в Университете.

4.10. Выполняет функции администраторов информационной безопасности Университета по предотвращению несанкционированного доступа лиц к защищаемой информации в информационных системах Университета.

4.11. Контролирует предоставление и отзыв прав доступа к информационным ресурсам в Университете.

4.12. Осуществляет мониторинг действий пользователей в процессе их работы в информационных системах Университета.

4.13. Учитывает и контролирует события, связанные с информационной безопасностью Университета.

4.14. Контролирует удаленный доступ к информационной инфраструктуре Университета.

4.15. Контролирует настройки сетевого оборудования в соответствии с требованиями информационной безопасности Университета.

4.16. Контролирует состояния антивирусной защиты информационных систем Университета.

4.17. Осуществляет мониторинг действий пользователей в информационных системах Университета.

4.18. Участвует в действиях по восстановлению работоспособности оборудования, обеспечивающего информационную безопасность Университета, после сбоев и аварий.

4.19. Согласовывает технические задания, проектную и другую техническую документацию на вновь создаваемые информационные системы или программное обеспечение, услуги в области информационных технологий в части выполнения требований по защите информации.



4.20. Осуществляет проведение плановых проверок режима защиты информации, обеспечивает разработку соответствующей документации, проводит анализ результатов и расследование нарушений.

4.21. Организует и проводит мероприятия по повышению осведомленности работников и обучающихся Университета по вопросам обеспечения информационной безопасности.

4.22. Обеспечивает информационную поддержку работников Университета по вопросам информационной безопасности.

4.23. Организует внедрение нормативных документов по обеспечению информационной безопасности в Университете.

4.24. Выполняет иные функции

## **5. Права подразделения**

С целью реализации функций отдел информационной и кибербезопасности имеет право:

5.1. Запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений Университета, необходимым для принятия решений по всем вопросам, отнесенным к компетенции отдела.

5.2. Готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности Университета, имеющих лицензии на соответствующий вид деятельности.

5.3. Контролировать деятельность структурных подразделений Университета по выполнению требований по обеспечению информационной безопасности.

5.4. Постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности.

5.5. Участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций.

5.6. Участвовать в работе комиссий Университета при рассмотрении вопросов обеспечения информационной безопасности.

5.7. Проводить плановые и внеплановые проверки структурных подразделений Университета по выполнению требований по обеспечению информационной безопасности.

5.8. Вносить предложения руководству Университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности.

5.9. Вносить представления руководству Университета в отношении работников при обнаружении фактов нарушения работниками Университета

установленных требований безопасности информации в Университете, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности.

5.10. Вносить на рассмотрение руководству Университета предложения по вопросам деятельности отдела.

## **6. Взаимоотношения и связи подразделения**

6.1. В своей деятельности отдел информационной и кибербезопасности осуществляет служебные взаимоотношения и поддерживает связи со всеми структурными подразделениями Университета с целью обмена информацией и документами, а также выполнения возложенных на отдел задач по обеспечению информационной безопасности Университета.

6.2. По указанию руководства отдел информационной и кибербезопасности осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по вопросам информационной безопасности.

## **7. Ответственность подразделения**

7.1. Ответственность за своевременное и качественное выполнение установленных настоящим Положением задач и функций несет начальник отдела информационной и кибербезопасности.

7.2. Степень ответственности работников отдела информационной и кибербезопасности указана в соответствующих должностных инструкциях.

Разработано:

Начальник отдела информационной и кибербезопасности



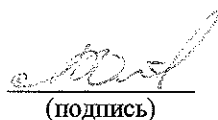
(подпись)

\_\_\_\_\_ (дата)

В.С. Чапрасов

Согласовано:

Советник по безопасности Ректората –  
исполняющий обязанности начальника  
управления безопасности



(подпись)

\_\_\_\_\_ (дата)

А.Т. Байков

**Лист ознакомления  
с положением об отделе информационной и кибербезопасности  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова**

<b>Должность</b>	<b>ФИО</b>	<b>Дата</b>	<b>Подпись</b>