МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Временно исполняющий обязанности ректора
_____ Д.В. Ярыгин
«15» 06 2026 г.
К приказу от «15» 06 2026 г.
№ 1463-к

ПОЛОЖЕНИЕ

о Центре информационной безопасности Дирекции информатизации и связи

Севастополь
2026

Содержание

1. Общие положения

1.1. Настоящее Положение регулирует деятельность Центре информационной безопасности (далее – Положение) Дирекции информатизации и связи (далее – Дирекции) федерального государственного автономного образовательного учреждения высшего образования «Севастопольский государственный университет» (далее – Университет) определяет основные задачи, функции, структуру и порядок организации деятельности Центра информационной безопасности (далее – Центр), а также порядок взаимодействия Центра с другими структурными подразделениями Университета и сторонними организациями.

1.2. Центр информационной безопасности является структурным подразделением Университета, входит в структуру Дирекции информатизации и связи и не является юридическим лицом.

1.3. Полное официальное наименование: Центр информационной безопасности Дирекции информатизации и связи федерального государственного автономного образовательного учреждения высшего образования «Севастопольский государственный университет».

Сокращенные наименования: Центр информационной безопасности; Центр ИБ.

1.4. Деятельность Центра осуществляется в соответствии с действующим законодательством Российской Федерации, в том числе Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании», Требования Федеральной службы по техническому и экспортному контролю о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений иными федеральными конституционными законами, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, другими нормативными правовыми актами, письмами Министерства науки и высшего образования Российской Федерации, Программой развития федерального государственного автономного образовательного учреждения высшего образования «Севастопольский государственный университет», Концепцией развития Севастопольского государственного университета, уставом Университета, решениями учёного совета Университета, приказами и распоряжениями ректора Университета (уполномоченного лица), проректора по цифровой трансформации, настоящим Положением и иными локальными нормативными актами Университета.

Дирекция правового обеспечения и внутреннего контроля
И.С. Магера

1.5. Термины и определения:

Компьютерная атака	– целенаправленное воздействие программных и (или) программно-аппаратных средств на информационную систему, информационно-телекоммуникационные сети, автоматизированную систему управления или сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;
Компьютерный инцидент	– факт нарушения и (или) прекращения функционирования информационной системы, информационно-телекоммуникационной сети, автоматизированной системы управления или сети электросвязи, используемых для организации взаимодействия таких объектов, и (или) нарушения безопасности информации, обрабатываемой этими объектами, в том числе произошедший в результате компьютерной атаки;
Объект информатизации	– информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть или иной объект информатизации;
Подрядная организация	– организация, которой предоставляется доступ к информационным системам Университета и (или) содержащейся в них информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации;
Угрозы безопасности информации	– совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

1.6. Сокращения:

ИС	– информационная система, включенная в перечень объектов, подлежащих защите в соответствии с Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117.
ИБ	- информационная безопасность;

Дирекция правового обеспечения и внутреннего контроля
И.С. Магера

ОИ	– объект информатизации;
СКЗИ	– средства криптографической защиты информации;
НКЦКИ	– Национальный координационный центр по компьютерным инцидентам;
СрЗИ	– средство защиты информации.

2. Цели и задачи деятельности Центра

2.1. Целью деятельности Центра является:

– исключение или существенное снижение негативных последствий (ущерба) для Университета вследствие нарушения функционирования его ИС в результате реализации угроз безопасности информации;

– повышение защищенности Университета от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования эксплуатируемых ИС Университета или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

– обеспечение надежности и эффективности функционирования и безопасности ИС Университета, рабочих мест пользователей ИС и других операторов, производственных процессов и информационно-технологической инфраструктуры Университета;

– обеспечение выполнения требований по информационной безопасности при создании и функционировании ИС Университета.

2.2. Деятельность Центра направлена на выполнение следующих задач:

– планирование, организация и координация работ по обеспечению информационной безопасности Университета и контроль за ее состоянием;

– выявление угроз безопасности информации и уязвимостей ИС, программного обеспечения и программно-аппаратных средств;

– предотвращение утечки 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 и его производственных процессов в случае проведения компьютерных атак;

– взаимодействие с НКЦКИ;

– нормативно-правовое обеспечение использования информационных ресурсов.

3. Функции Центра

Для решения задач, перечисленных в пункте 2.2 настоящего Положения, Центр осуществляет следующие функции и несет ответственность за их невыполнение:

3.1. Организация деятельности по обеспечению информационной безопасности:

3.1.1 Разработка и поддержание в актуальном состоянии локальных актов Университета по обеспечению информационной безопасности;

3.1.2 Ознакомление работников Университета с документами, определяющими политику информационной безопасности Университета и иными локальными нормативными актами Университета по обеспечению информационной безопасности в части, их касающейся;

3.1.3 Обеспечение применения сертифицированных средств защиты информации (СрЗИ), прошедших оценку соответствия требованиям Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании», с обязательной поддержкой безопасности разработчиком на территории Российской Федерации и неукоснительным соблюдением требований и ограничений, установленных Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

3.1.4 Осуществление учета и контроля СКЗИ, включая регистрацию экземпляров, ключевых документов, а также проверку целостности и соблюдения условий эксплуатации;

3.1.5 Разработка предложений по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий по обеспечению информационной безопасности;

3.1.6 Ознакомление подрядных организаций с локальными нормативными актами Университета по обеспечению информационной безопасности в части, их касающейся;

3.1.7 Обеспечение контроля работников Университета по соблюдению требований нормативных и иных документов по обеспечению ИБ;

3.1.8 Совершенствование системы обеспечения ИБ в Университете;

3.1.9 Обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения негативных последствий (невозможности реализации) путем разработки и реализации организационных мер и применения СрЗИ;

3.2. Проведение мероприятий и принятие мер по обеспечению информационной безопасности:

3.2.1. Организация развития навыков безопасного поведения по вопросам обеспечения информационной безопасности Университета, в том числе проведение занятий с руководящим составом и специалистами Университета;

3.2.2. Выполнение иных функций, исходя из поставленных руководством Университета целей и задач в рамках обеспечения информационной безопасности Университета, подведомственных органов (организаций) (при наличии).

3.3. Проведение оценки состояния защиты информации на основе представленных данных Отделом защиты информации:

3.3.1. Периодический (не реже 1 раза в 3 года) контроль за обеспечением безопасности ОИ;

3.3.2. Контроль (анализ) защищенности ОИ с учетом особенностей его

Дирекция правового обеспечения и внутреннего контроля

И.С. Магера

функционирования;

3.3.4. Документирование процедур и результатов контроля за обеспечением безопасности ОИ.

3.4. Совершенствование мероприятий и мер по защите информации.

3.5. Планирование мероприятий и мер, направленных на обеспечение информационной безопасности.

3.6. Подготовка отчетов о состоянии работ по обеспечению информационной безопасности Университета.

4. Организационная структура Центра

4.1. Центр является структурным подразделением Университета и входит в состав Дирекции информатизации

В состав Центра входит следующее структурное подразделение:

– Отдел защиты информации.

Количество структурных подразделений может изменяться на основании приказа ректора.

4.2. Деятельность работников Центра регламентируется должностными инструкциями.

4.3. Штатное расписание Центра разрабатывается и утверждается в установленном в Университете порядке.

4.4. Трудовые отношения работников Центра регулируются законодательством Российской Федерации о труде и локальными нормативными актами Университета.

4.5. Центр создаётся, переименовывается, реорганизуется и ликвидируется приказом ректора Университета.

5. Руководство Центром

5.1. Общее руководство и координацию деятельности Центра осуществляет директор Дирекции.

5.2. Непосредственное руководство Центром осуществляет директор Центра, который назначается на должность и освобождается от нее приказом ректора Университета по представлению директора Дирекции.

5.3. На должность директора Центра назначается лицо, в соответствии с квалификационными требованиями, установленными должностной инструкцией.

5.4. Директор Центра осуществляет свою деятельность в соответствии с действующим законодательством Российской Федерации, должностной инструкцией и трудовым договором.

5.5. Директор Центра исполняет следующие обязанности:

5.5.1. Осуществляет руководство деятельностью Центра, обеспечивает организацию его работы, выполнение задач, определённых настоящим Положением, руководствуясь действующими нормативными документами, решениями наблюдательного совета, решениями учёного совета, приказами и распоряжениями ректора или уполномоченного им лица.

5.5.2. Определяет цели, задачи, стратегию развития Центра.

5.5.3. Организовывает текущее и перспективное планирование деятельности Центра с учётом целей, задач и направлений его деятельности.

5.5.4. Разрабатывает проекты документов по вопросам организационного сопровождения деятельности Центра, вносит их на рассмотрение и утверждение в установленном порядке.

5.5.5. Контролирует и принимает меры по соблюдению работниками Центра при исполнении ими своих должностных обязанностей законодательства Российской Федерации, Устава и локальных нормативных актов Университета, в том числе Правил внутреннего трудового распорядка Университета, правил охраны труда, техники безопасности, производственной санитарии, пожарной безопасности и трудовой дисциплины.

5.5.6. Осуществляет подбор, расстановку и перемещение работников Центра.

5.5.7. Распределяет обязанности между работниками Центра в рамках функциональных обязанностей, определённых их должностными инструкциями.

5.5.8. Контролирует своевременное и качественное исполнение работниками Центра приказов (распоряжение) и поручений ректора, проректора по цифровой трансформации, распоряжений и поручений директора Дирекции; решений коллегиальных органов управления Университета.

5.5.9. Осуществляет контроль за состоянием делопроизводства в Центре в соответствии с Инструкцией по делопроизводству и Номенклатурой дел в Университете.

5.5.10. Разрабатывает проекты локальных нормативных актов по направлениям деятельности Центра и представляет их на утверждение в установленном порядке.

5.5.11. Организует работу по осуществлению взаимодействия со структурными подразделениями Университета по вопросам, входящим в компетенцию Центра.

5.5.12. Организует работу по подготовке проектов писем, заявлений, ходатайств, жалоб, обращений и другой корреспонденции по вопросам, входящим в компетенции Центра.

5.5.13. Подготавливает и своевременно представляет в установленном порядке справочные, аналитические, информационные материалы и отчетную документацию о деятельности Центра.

5.5.14. Согласовывает документы в пределах представленных полномочий.

5.5.15. Разрабатывает и вносит предложения проректору по цифровой трансформации и директору Дирекции по совершенствованию системы обеспечения ИБ.

5.5.16. Подготавливает и представляет на рассмотрение руководству проекты документов по вопросам обеспечения ИБ.

5.5.17. Принимает участие в создании и поддержке систем автоматизации, антивирусной безопасности, обновлений и учета программного обеспечения.

5.5.18. Осуществляет планирование, организацию и координацию работ по обеспечению информационной безопасности Университета и контроль за ее состоянием.

5.5.19. Организует и контролирует деятельность по:

– выявлению угроз безопасности информации и уязвимостей ИС, программного обеспечения и программно-аппаратных средств;

– предотвращению утечки 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;

– поддержанию стабильной деятельности Университета и его производственных процессов в случае проведения компьютерных атак;

5.5.20. Осуществляет взаимодействие с НКЦКИ.

5.5.21. Предоставляет работникам Университета консультации и разъяснения по вопросам, входящим в компетенцию Центра.

5.5.22. Повышает свой профессиональный уровень. Осуществляет мониторинг нормативных правовых актов по направлениям своей деятельности.

5.5.23. Исполняет иные обязанности определенные его должностной инструкцией, в соответствии с действующим законодательством Российской Федерации, уставом Университета, решениями наблюдательного и учёного совета Университета, приказами (распоряжениями) и поручениями ректора, проректора по цифровой трансформации, распоряжениями и поручениями директора Дирекции.

5.6. Директор Центра имеет право:

5.6.1. Знакомиться с решениями руководства Университета, касающимися его деятельности.

5.6.2. Запрашивать и получать от структурных подразделений Университета сведения, справочные и другие материалы, необходимые для выполнения своих должностных обязанностей.

5.6.3. Знакомиться с локальными нормативными актами Университета, устанавливающими порядок обеспечения информационной безопасности, обеспечения безопасности критической информационной инфраструктуры в Университете.

5.6.4. Требовать от работников Университета соблюдения требований законодательства Российской Федерации и локальных нормативных актов Университета, устанавливающих порядок обеспечения безопасности критической информационной инфраструктуры в Университете.

5.6.5. Вносить свои предложения по совершенствованию мероприятий и мер по вопросам обеспечения информационной безопасности, обеспечения безопасности критической информационной инфраструктуры в Университете, участвовать в проведении таких мероприятий.

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

5.6.7. Вносить представления руководству Университета в отношении работников Университета при обнаружении фактов нарушения работниками установленных требований безопасности информации Университета, в том числе ходатайствовать о привлечении указанных работников к ответственности.

5.6.8. Вносить на рассмотрение проректору по цифровой трансформации и директора Дирекции предложения по совершенствованию работы Центра.

5.6.9. В пределах своей компетенции сообщать проректору по цифровой трансформации и директору Дирекции и о всех выявленных в процессе деятельности Центра недостатках и вносить предложения по их устранению.

5.6.10. Пользоваться информационными ресурсами Университета для осуществления функций, возложенных на Центр.

5.6.11. Пользоваться другими правами, предусмотренными законодательством Российской Федерации, уставом и локальными нормативными актами Университета, Коллективным договором.

5.7. Директор Центра несёт ответственность за:

5.7.1. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящим Положением и должностной инструкцией, – в пределах, определённых действующим трудовым законодательством Российской Федерации.

5.7.2. Нарушение Устава Университета, Правил внутреннего трудового распорядка, локальных нормативных актов Университета, в том числе в сфере противодействия коррупции, правил охраны труда и требований пожарной безопасности – в пределах, определённых законодательством Российской Федерации.

5.7.3. Неисполнение или ненадлежащее исполнение задач и функций, возложенных на Центр.

5.7.4. Последствия принимаемых им решений и состояние порученных ему направлений работы.

5.7.5. Недостоверность и неполноту информации, представляемой ректору Университета, проректору по цифровой трансформации и директору Дирекции, а также за несвоевременное и ненадлежащее выполнение приказов (распоряжений) и поручений ректора Университета либо уполномоченного им лица, проректора по цифровой трансформации, распоряжений и поручений директора Дирекции.

5.7.6. Ненадлежащую организацию делопроизводства в Центре.

5.7.7. Причинение материального ущерба – в пределах, определённых трудовым и гражданским законодательством Российской Федерации.

5.7.8. Правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определённых административным, уголовным и гражданским законодательством Российской Федерации.

Дирекция правового, гражданского и внутреннего контроля
И.С. Магера

5.7.9. Разглашение охраняемой законом тайны, а также сведений, ставших ему известными в связи с исполнением должностных обязанностей, персональных данных работников и иных лиц – в порядке, установленном действующим законодательством Российской Федерации.

6. Порядок работы, оплаты труда, права, обязанности и ответственность работников Центра

6.1. Работники Центра назначаются на должность приказом ректора Университета либо уполномоченного им лица по представлению директора Дирекции. С работниками заключается трудовой договор.

6.2. Права, обязанности, ответственность и требования к квалификации работников Центра определяются соответствующими должностными инструкциями, утверждёнными в установленном в Университете порядке, и трудовыми договорами.

6.3. Работники Центра выполняют свои обязанности в соответствии с должностными инструкциями, распоряжениями и поручениями проректора по цифровой трансформации, директора Дирекции и директора Центра, локальными нормативными актами Университета.

6.4. Трудовые отношения работников Центра регулируются законодательством Российской Федерации о труде.

6.5. Должностной оклад устанавливается в соответствии с формой и системой оплаты труда, принятой в Университете. Оплата труда работников Центра может включать в себя выплаты стимулирующего характера, доплаты, надбавки, установленные локальными нормативными актами Университета.

6.6. Работники Центра должны повышать квалификацию в области своей профессиональной деятельности.

6.7. Продолжительность и распорядок рабочего дня, порядок предоставления выходных дней, отпусков и другие вопросы трудовой деятельности работников Центра регулируются действующим законодательством Российской Федерации, Правилами внутреннего трудового распорядка и иными локальными нормативными актами Университета.

6.8. Работники Центра несут ответственность за:

- неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных должностной инструкцией;
- несвоевременное и некачественное исполнение приказов (распоряжений) ректора либо уполномоченного лица, проректора по цифровой трансформации, распоряжений и поручений директора Дирекции и Центра;
- недостоверность и неполноту информации, предоставляемой проректору по цифровой трансформации и директору Дирекции, директору Центра;
- разглашение охраняемой законом тайны, сведений, ставших им известными в связи с исполнением должностных обязанностей, персональных

Дирекция правового обеспечения и внутреннего контроля
И.С. Магера

данных работников и иных лиц – в порядке, установленном действующим законодательством Российской Федерации.

7. Взаимодействие с другими подразделениями

7.1. Центр в различных формах взаимодействует со структурными подразделениями Университета, организациями, учреждениями и физическими лицами по вопросам своей деятельности в целях решения возложенных на него задач и функций.

7.2. Центр взаимодействует с ФСБ России, ФСТЭК России и Минцифрой России по указанию (или на основании поручения) руководства Университета.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения ректором Университета.

8.2. Внесение изменений или дополнений в настоящее Положение осуществляется путем подготовки изменений, дополнений или принятия положения в новой редакции.

8.3. Изменения или дополнения к настоящему Положению утверждаются приказом ректора Университета.

8.4. Подлинный экземпляр настоящего Положения подлежит регистрации и хранению в составе документов организационного характера в Отделе делопроизводства и архивного обеспечения Университета до замены его положением в новой редакции. Заверенная копия Положения хранится в составе документов организационного характера.